Saludos a todos en la lista CrackSlatinos, y bueno en vista de practicar las primeras lecciones del profesor Ricardo me di a la tarea de buscar un programa que no fueran los Crackme, para probarme a ver que tanto había aprendido y en unos de los mail del grupo CracSlatinoS que me llego leí algo sobre un problema que tenía un listero para utilizar la captura de imágenes del Olly, buscando por la red encontré este que se adapto sin querer a las necesidades del listero y mías, jejejeje mate un pájaro de un tiro.

ATENCION

ES IMPORTANTE ENTENDER QUE ESTE TUTORIAL NO FUE ESCRITO CON CARÁCTER DE FOMENTAR LA PIRATERIA SINO UNICA Y EXCLUSIVAMENTE CON FINES EDUCATIVOS. QUIEN LO UTILIZE CON OTRO PROPOSITO QUEDA BAJO SU EXTRICTA RESPONSABILIDAD.

TAREA:

Víctima:	Cool Capture
Versión:	V1.25
URL:	http://www.sharewareconnection.com/download-cool-capture-from-sharecon.html
Protección:	Serial + 30 días de uso
Dificultad:	Newbie Avanzado
Herramientas:	RDG Packer Detector, OllyDbg.
Compilador:	Microsoft Visual C++ V6.0
Cracker:	CORNEL065

DATOS DE LA VICTIMA

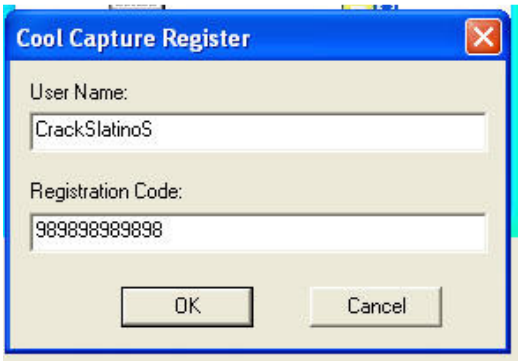
Cool Capture is an all-in-one soft for free screen capture. You can capture screen in many ways, including full screen capture, region capture, window capture, scroll capture and etc.Using a hot key or a button, you can copy a window, an area, or a scrolling Web page and send it to the clipboard, a file, or your favorite graphics application.In the near future, this tool will support video screen capture, sound capture. You can choose many kinds of output ways, including clipboard, printer, editor tool and all popular formats. Cool Capture has an easy-to-use and intuitive interface. Whatever you can see on your screen,Cool Capture will easily and fastest capture for your immediate use. More Than 6 Ways to Capture. Easy-to-Use and Intuitive Interface. More Than 6 Ways to Output. Setup Custom Hotkeys for Any Way. Support all popular Internet formats. Support Down Scroll, Right Scroll ,Full Scroll Capture.You can choose the program to edit the picture.

AL ATAKE MIS CAMARADAS!!!!

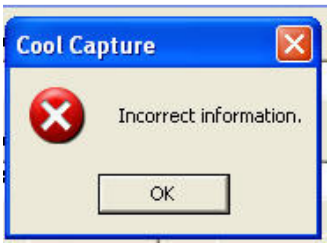
Este programa es muy sencillo de usar e instalar y al correrlo nos sale una nag como la siguiente:

Ya de entrada nos invita a registrarnos y nos dice que solo tenemos 30 días de uso, y nos muestra un corazoncito para enamorarnos y comprarlo, si como no jejejeje.

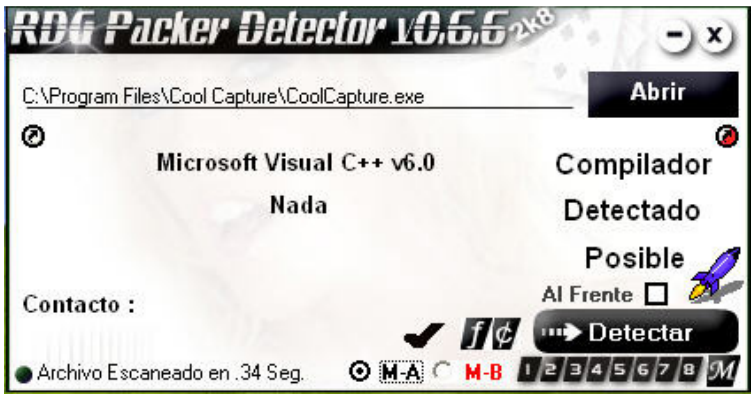
A mi me quedan solo 28 dias, bueno voy a probar suerte, hago clic en **Enter Register** y coloco los siguientes datos.



Doy clic en Ok.

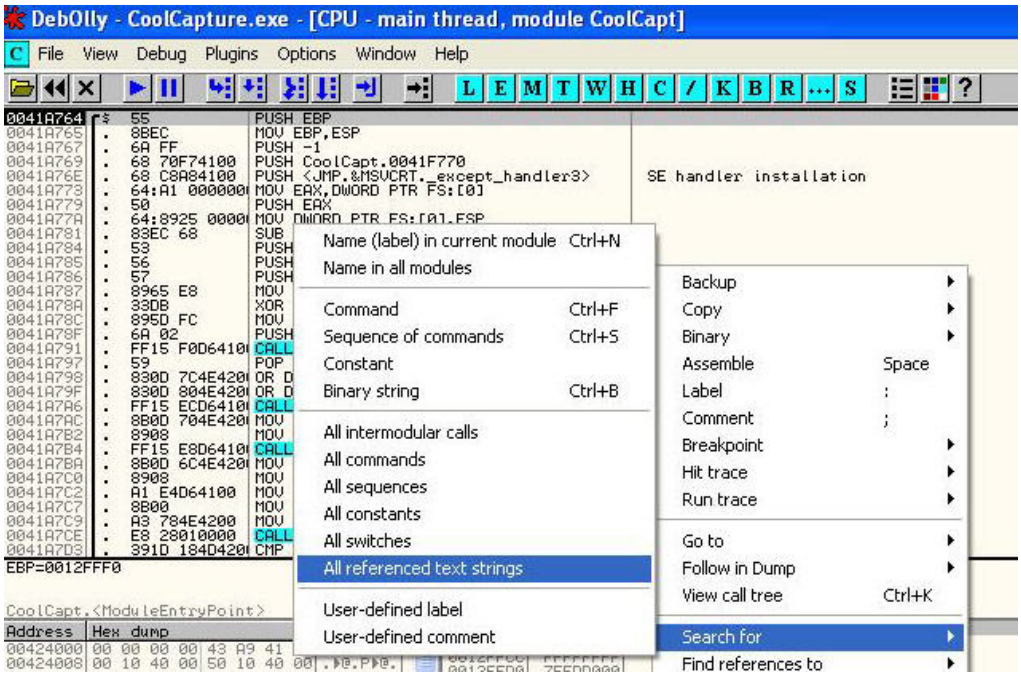


Grrr. Carajo me salió el cartelito del chico malo no la pegue jejeje bueno al menos me dio un dato de que buscar, así que me lo cargo con el muy humilde OllyDbg a ver que nos dice. Ahh pero antes y siguiendo siempre el ejemplo de los expertos lo analizo a ver si viene encriptado asi que le paso el amigo RDG Packer Detector.

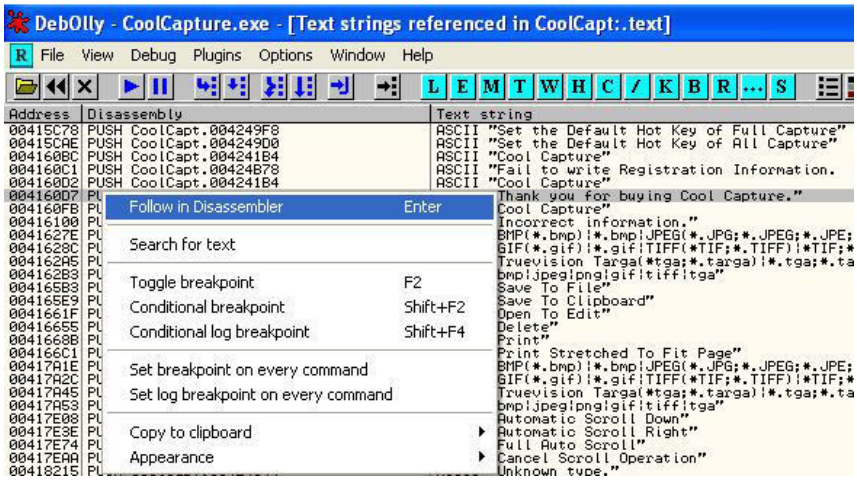


Guao!!!! que bien tuve suerte jejejeje, esta limpiecito. Ahora si voy con el OllyDbg.

Me cae en el EP, y sin perder un instante me voy a buscar la cadena de textos que mostro el cartelito anterior.



Como que ando de suerte porque mostro los chicos buenos y malos así que voy directo a esas direcciones a ver qué puedo hacer.




```
00416093  .  C68424 CC010( MOV BYTE PTR SS:[ESP+1CC],0
0041609B  .  8B48 04       MOV ECX,DWORD PTR DS:[EAX+4]
0041609E  .  89540C 14     MOV DWORD PTR SS:[ESP+ECX+14],EDX
004160A2  .  A1 48D64100   MOV EAX,DWORD PTR DS:[<&MSVCP60.??_7?$b
004160A7  .  8D4C24 6C     LEA ECX,DWORD PTR SS:[ESP+6C]
004160AB  .  894424 6C     MOV DWORD PTR SS:[ESP+6C],EAX
004160AF  .  FF15 4CD6410( CALL DWORD PTR DS:[<&MSVCP60.??1ios_bas  MSVCP60.??1ios_base@std@@UAE@XZ
004160B5  .v EB 16         JMP SHORT CoolCapt.004160CD
004160B7  >  8B4F 20       MOV ECX,DWORD PTR DS:[EDI+20]
004160BA  .  6A 10         PUSH 10                                  Style = MB_OK|MB_ICONHAND|MB_APPLMODAL
004160BC  .  68 B4414200   PUSH CoolCapt.004241B4                   Title = "Cool Capture"
004160C1  .  68 784B4200   PUSH CoolCapt.00424B78                   Text = "Fail to write Registration Information.
004160C6  .  51            PUSH ECX                                 hOwner
004160C7  .  FF15 78D7410( CALL DWORD PTR DS:[<&USER32.MessageBoxA  MessageBoxA
004160CD  >  8B57 20       MOV EDX,DWORD PTR DS:[EDI+20]
004160D0  .  6A 00         PUSH 0                                   Style = MB_OK|MB_APPLMODAL
004160D2  .  68 B4414200   PUSH CoolCapt.004241B4                   Title = "Cool Capture"
004160D7  .  68 544B4200   PUSH CoolCapt.00424B54                   Text = "Thank you for buying Cool Capture."
004160DC  .  52            PUSH EDX                                 hOwner
004160DD  .  FF15 78D7410( CALL DWORD PTR DS:[<&USER32.MessageBoxA  MessageBoxA
004160E3  .  C605 504E420( MOV BYTE PTR DS:[424E50],1
004160EA  .  8B07          MOV EAX,DWORD PTR DS:[EDI]
004160EC  .  8BCF          MOV ECX,EDI
004160EE  .  FF90 CC00000( CALL DWORD PTR DS:[EAX+CC]
004160F4  .v EB 16         JMP SHORT CoolCapt.0041610C
004160F6  >  8B4F 20       MOV ECX,DWORD PTR DS:[EDI+20]
004160F9  .  6A 10         PUSH 10                                  Style = MB_OK|MB_ICONHAND|MB_APPLMODAL
004160FB  .  68 B4414200   PUSH CoolCapt.004241B4                   Title = "Cool Capture"
00416100  .  68 3C4B4200   PUSH CoolCapt.00424B3C                   Text = "Incorrect information."
00416105  .  51            PUSH ECX                                 hOwner
00416106  .  FF15 78D7410( CALL DWORD PTR DS:[<&USER32.MessageBoxA  MessageBoxA
0041610C  >  8D8C24 A0000( LEA ECX,DWORD PTR SS:[ESP+A0]
00416113  .  C78424 CC010( MOV DWORD PTR SS:[ESP+1CC],-1
0041611E  .  E8 9DACFFFF   CALL CoolCapt.00410DC0
00416123  .  8B8C24 C4010( MOV ECX,DWORD PTR SS:[ESP+1C4]
0041612A  .  5F            POP EDI
0041612B  .  5E            POP ESI
0041612C  .  5D            POP EBP
0041612D  .  64:890D 0000( MOV DWORD PTR FS:[0],ECX
00424B54=CoolCapt.00424B54 (ASCII "Thank you for buying Cool Capture.")
```

Está saliendo a pedir de boca jejeje, me muestra sus más íntimos secretos, ya entiendo lo del corazoncito, bueno como les dije me voy al texto del cartelito malo que salió al meter una clave incorrecta **Incorrect Information**

```
004160EE  .  FF90 CC00000( CALL DWORD PTR DS:[EAX+CC]
004160F4  .v EB 16         JMP SHORT CoolCapt.0041610C
004160F6  >  8B4F 20       MOV ECX,DWORD PTR DS:[EDI+20]
004160F9  .  6A 10         PUSH 10                                  Style = MB_OK|MB_ICONHAND|MB_APPLMODAL
004160FB  .  68 B4414200   PUSH CoolCapt.004241B4                   Title = "Cool Capture"
00416100  .  68 3C4B4200   PUSH CoolCapt.00424B3C                   Text = "Incorrect information."
00416105  .  51            PUSH ECX                                 hOwner
00416106  .  FF15 78D7410( CALL DWORD PTR DS:[<&USER32.MessageBoxA  MessageBoxA
0041610C  >  8D8C24 A0000( LEA ECX,DWORD PTR SS:[ESP+A0]
Jump from 00415EAC
```

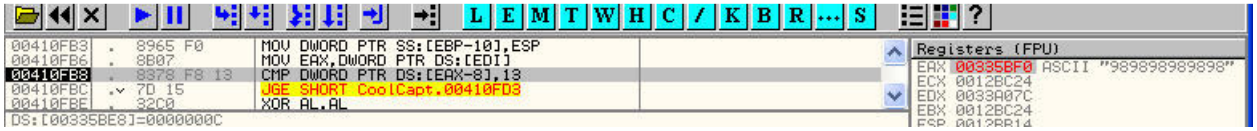
En la dirección 4160F6 es donde empieza a generarse dicho cartel, pero el Olly me indica también con una flechita de donde viene, y si leemos más abajo observamos la dirección exacta que es la 415EAC así que haya voy.

```
00415EA5  .  E8 E6B0FFFF   CALL CoolCapt.00410F90
00415EAA  .  84C0          TEST AL,AL
00415EAC  .v 0F84 4402000( JE CoolCapt.004160F6
00415EB2  .  8D8424 C0000( LEA EAX,DWORD PTR SS:[ESP+C0]
00415EB9  .  68 04010000   PUSH 104
```

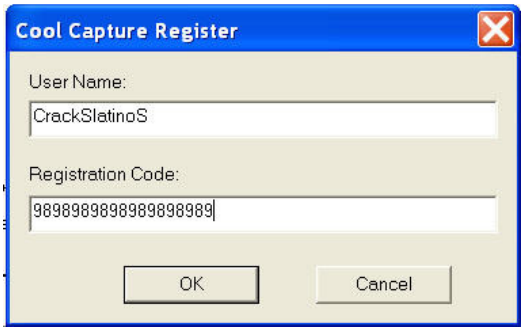
Interesante lo que nos dice nuestro amiguito en esas tres instrucciones a partir de 415EA5 con el Call, el Test y el Je, si al testear AL con Al da cero el salto Je nos

manda para el carajo (chico malo), esto implica que dentro de esa llamada hay algo que podría salvarnos la vida, miremos que hay dentro.

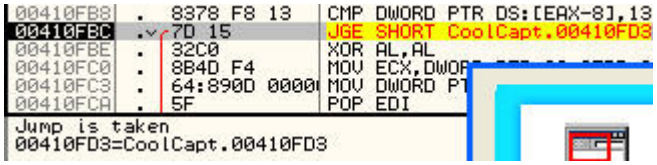
Corriendo un poco dentro de la call **415EA5** con F7 me encuentro con algo muy interesante y es una comparación de mi clave con 13 hex que en decimal seria 19 en la dirección **410FB6.**



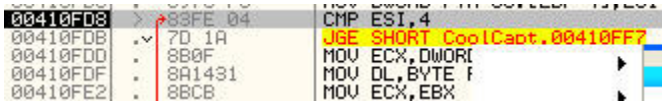
Según los cálculos del programa la clave que introduje da C en hex, esto en decimal es 12 por lo tanto no lleno los requisitos y me manda al chico malo, bueno acepto pero para la próxima tengo la precaución de meter 19 números.



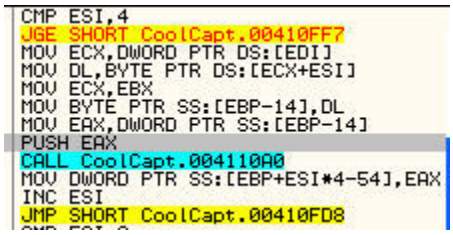
Miramos nuevamente y bieeeeen!!!! Ganamos, tenemos un poco mas de vida jejejejeje. Pasamos la comprobación veremos a donde nos manda.



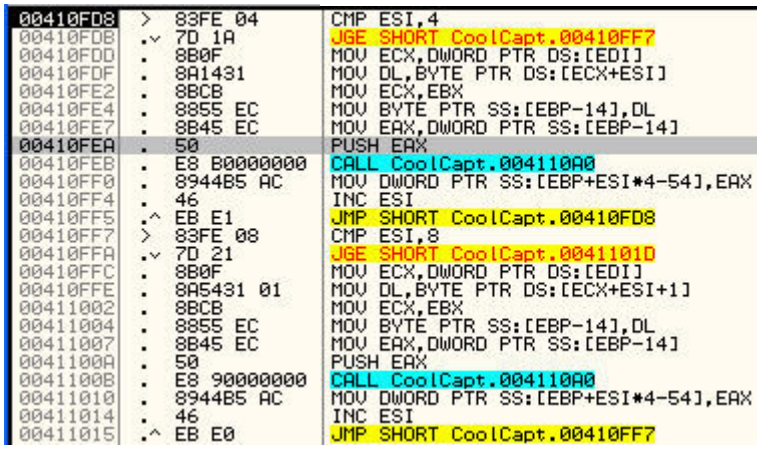
Caemos aquí en la dirección 410FD8 y carga el registro ESI con 4 para qué es esto?



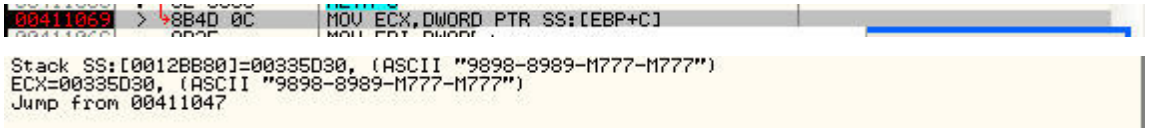
Recorriendo estas instrucciones lo que realmente hace es que toma los 4 primeros números de mi serial y los almacena, el registro ESI funciona como un contador, en la imagen de abajo se puede apreciar con mas claridad este proceso asi que lo corremos y seguimos con F7.



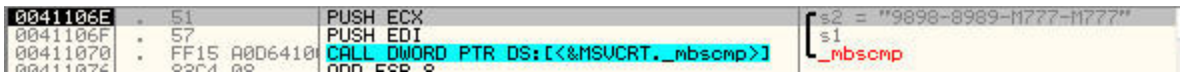
Después del programa tomar los 4 primeros dígitos continua con los 4 siguientes, por ejemplo ya tomo 9898. Ahora va por los otros cuatros pero aquí hay algo interesante al hacer los incrementos con ESI el deja el quinto puesto y no introduce el numero, que significa esto que empieza a tomarlos después del 6to por ejemplo 8989, lo legal seria 9898 pero no los toma así. Esto se puede apreciar con la instrucción con dirección 410FF7 donde carga el contador con 8.



Y bueno después de pasar la rutina anterior y tomar los datos mencionados continuando con F7 caemos en esta dirección de memoria 411069 mi amiguito OllyDb me muestra algo como que pasa los datos apuntado por EBP+C a ECX y también nos dice que datos son eso, joder eso como que parece una clave jejejejejeje bueno esta victima ya murió. Los datos son 9898-8989-M777-M777.



Ok con estos datos busco lápiz y papel y los anoto, pero continuemos con F7, a ver a donde nos lleva el OllyDbg, después de recorrer algunas instrucciones nos confirma sobre la clave anterior con esta librería de comparación mbscmp miremos a ver con que lo compara doy f7 nuevamente y.



Aquí nos muetra la clave que metimos, bueno ya sabemos el resultado de esta comparación, asi que doy F9 acepto el mensaje de error y escribo la clave buena.

Hago clic en Ok y taran tarannn estoy registradoooooo jejejejeje

Bueno me gustaría hacer un keygen pero aun estoy investigando como forma esa clave espero para la próxima hacerlo, claro le pediré ayuda al buen amigo Thunder que los confecciona muy bien, si alguien lo quiere hacer bien venido sea.

en fin este tutorial va dedicado a una buena amiga que empezó su carrera de ingeniería informática y le hable sobre el grupo espero la acepten aquí y así como también a todos los newbies y listeros que con esfuerzo tratan de entender el tema y se dieron a la tarea de leerlo.

Agradecimientos

Para las mejores metes brillantes el profesor Ricardo Narvaja por escribir tremendas teorías y facilitarlas sin pedir nada a cambio a Daniel, Raton, Guillermo, al Thunder por sus magníficos escritos, Zelt@ , +NCR/CRC!, MCKSys Argentina, CIS | ShaDDy, y si se me escapa alguno espero me perdone espero les guste este mi primer tutorial.