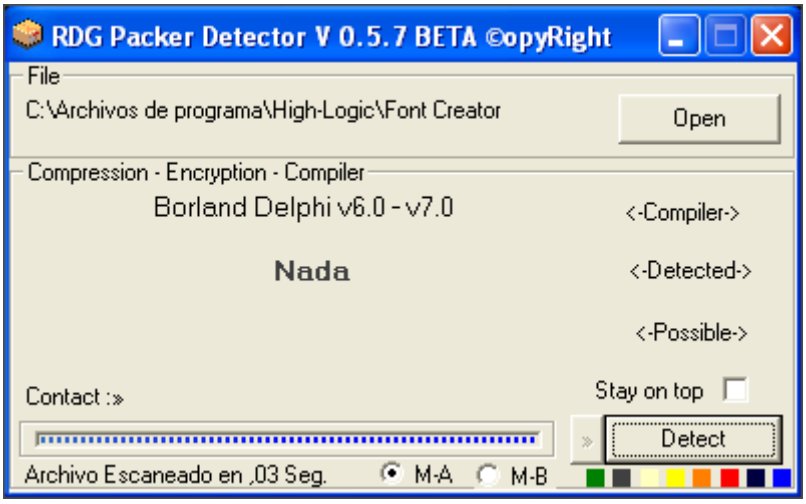
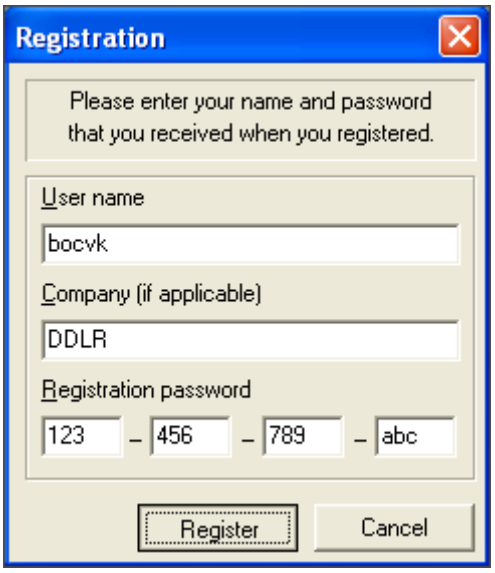
Instalamos el programa , luego tomamos a nuestra victima y la analizamos con el RDG. Para esto haremos click en Open y buscamos nuestro programa, luego haremos click en Abrir, y despu?s en Detect:

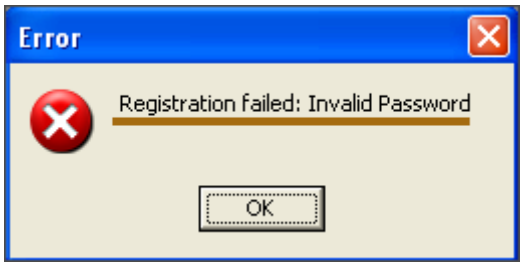


Como vemos el programa fu? compilado con Borland Delphi y no est? empacado, cosa que nos facilita el trabajo.

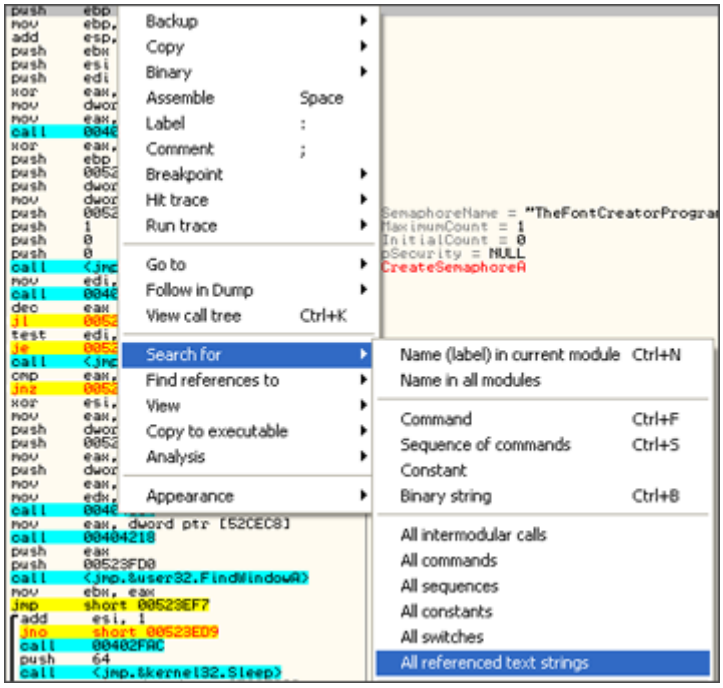
Ejecutamos el programa , y nos aparece una ventana con un boton para registrarnos , hacemos click y nos aparece otra ventana para poner algunos datos, llenemoslos :



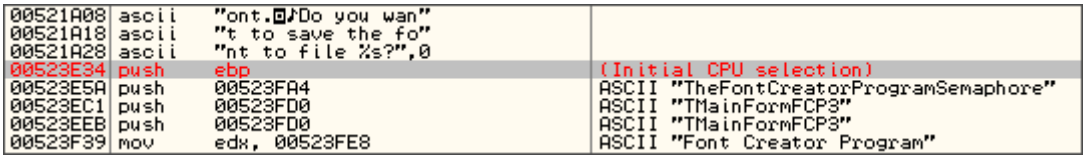
Le damos al boton Register , y nos aparece el Chico Malo diciendonos que la password ingresada es incorrecta, asi que apuntemos lo que nos aparece en algun bloc de notas :



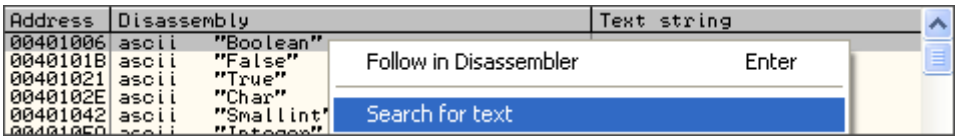
Abrimos el OllyDbg, y cargamos nuestro programa; en seguida haremos click derecho y vamos a Search For + All referenced text strings:

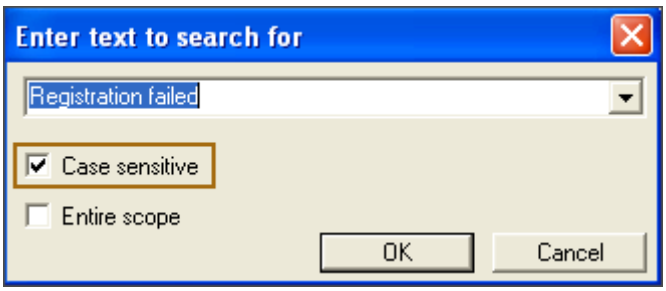


Aparecemos aqu? :



Nos vamos hacia la primera linea y haremos anticlick , luego click en Search for text e introducimos las 2 primeras palabras del chico malo "Registration failed", y marcamos donde dice Case sensitive , luego presionamos el boton Ok:





Aparecemos aqu? :

```
004F5544  ascii   "RegData",0
004F5650  mov     eax, 004F56EC          ASCII "Thank you for registering Font Creator Program."
004F5671  mov     eax, 004F5724          ASCII "Registration failed: Invalid Password"
004F56EC  ascii   "Thank you for re"
004F56FC  ascii   "gistering Font C"
```

Hacemos doble click donde habiamos aparecido para ir a la parte de c?digo donde se encuentran las instrucciones del chico malo, y luego caemos aqui :

```
004F564E  .  B2 02         mov     dl, 2
004F5650  .  B8 EC564F00   mov     eax, 004F56EC          ASCII "Thank you for registering Font Creator
004F5655  .  E8 E650F6FF   call    0045A740               FCP3.0045A740
004F565A  .  C783 3402000( mov     dword ptr [ebx+234], 1
004F5664  .v EB 1F         jmp     short 004F5685
004F5666  >  6A 00         push    0                      Chico Bueno
004F5668  .  66:8B0D E056( mov     cx, word ptr [4F56E0]
004F566F  .  B2 01         mov     dl, 1                  Arg1 = 00000000
004F5671  .  B8 24574F00   mov     eax, 004F5724          Chic
004F5676  .  E8 C550F6FF   call    0045A740               ASCII "Registration failed: Invalid Password"
                                                          FCP3.0045A740
```

Ahora iremos subiendo un poco hasta encontrar el simbolo ">", que nos indica que alli es donde se inician las sentencias de la llamada. Despu?s de encontrarlo pondremos un BreakPoint con F2:

```
004F55D8  .v 72 05         jb      short 004F55DF
004F55DA  .  E8 C5D9F0FF   call    00402FA4
004F55DF  >  42            inc     edx
004F55E0  .  8A4410 FF     mov     al, byte ptr [eax+edx-1]
004F55E4  .  50            push    eax
004F55E5  .  8D55 E0       lea     edx, dword ptr [ebp-20]
004F55E8  .  8B83 E0020000 mov     eax, dword ptr [ebx+2E0]
```

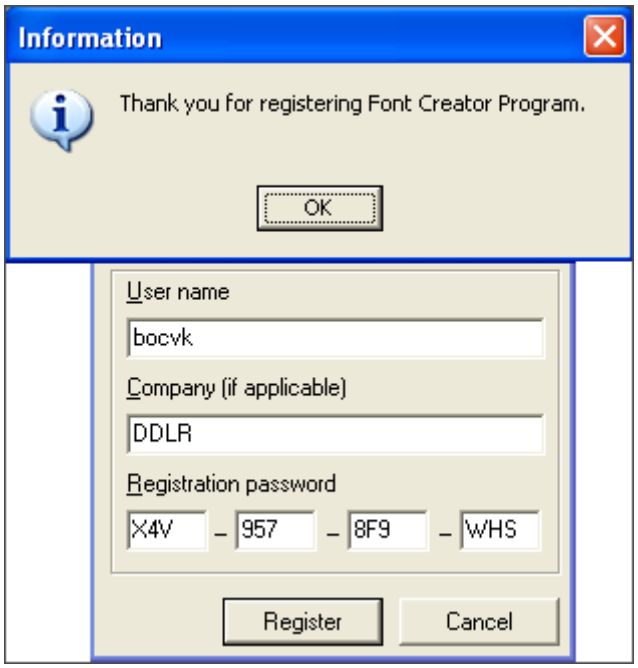
Lo que nos toca ahora es ejecutar el programa con F9, introducir los datos en la ventana de registro (colocamos los mismo que al principio), presionar el boton Register y el programa romper? en donde pusimos el BreakPoint:

```
004F55DA  .  E8 C5D9F0FF   call    00402FA4
004F55DF  >  42            inc     edx
004F55E0  .  8A4410 FF     mov     al, byte ptr [eax+edx-1]
004F55E4  .  50            push    eax
004F55E5  .  8D55 E0       lea     edx, dword ptr [ebp-20]
004F55E8  .  8B83 E0020000 mov     eax, dword ptr [ebx+2E0]
004F55EE  .  E8 99F7F3FF   call    00434D8C
004F55F3  .  8B45 E0       mov     eax, dword ptr [ebp-20]
004F55F6  .  8D4D E8       lea     ecx, dword ptr [ebp-18]
004F55F9  .  5A            pop     edx                    Traceamos
004F55FA  .  E8 8DF7FFFF   call    004F4D8C
004F55FF  .  8B45 E8       mov     eax, dword ptr [ebp-18]
004F5602  .  50            push    eax
```

Ahora traceamos con F8 hasta donde indique en la imagen anterior y vemos en la ventana de Informaci?n Adicional algo sospechoso :

```
004F55EE  .  E8 99F7F3FF   call    00434D8C
004F55F3  .  8B45 E0       mov     eax, dword ptr [ebp-20]
004F55F6  .  8D4D E8       lea     ecx, dword ptr [ebp-18]
004F55F9  .  5A            pop     edx
004F55FA  .  E8 8DF7FFFF   call    004F4D8C
004F55FF  .  8B45 E8       mov     eax, dword ptr [ebp-18]
004F5602  .  50            push    eax
004F5603  .  8D55 DC       lea     edx, dword ptr [ebp-24]
Stack ss:[0012EBE4]=00CA1804, (ASCII "X4U9578F9WHS")
eax=0012EBB4
```

Copiamos lo que encontramos , cerramos el OllyDbg y nos vamos a ejecutar el programa , lo que encontramos lo ponemos como serial :



Ya estamos registrados ... espero que hayan aprendido algo
Hasta la proxima
Salu2
Bocvk