Victima:	CCleaner Professional
Versión:	V5.26.5937
URL:	http://download.piriform.com/ccsetup526pro.exe
Protección:	TRIAL VERSION (14 DIAS DE PRUEBA)
Dificultad:	---------
Herramientas:	OLLYDBG v1.10 / RDG Packer Detector v0.7.6 2017 / Resource Hacker v4.5.30 / DUP 2
Objetivos	Crear un Parche para esta versión.
Reverser	L1oR
Lugar / Fecha:	Perú – Lima / 09/02/2017

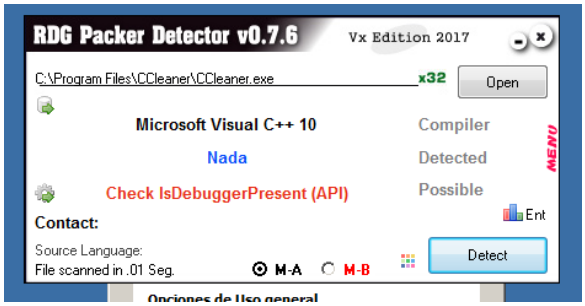
Información de Victima

Ccleaner es la herramienta número uno para limpiar los Equipos, protege su privacidad y hace que su computadora sea más rápida y segura. Es un copy y page de la web XD.

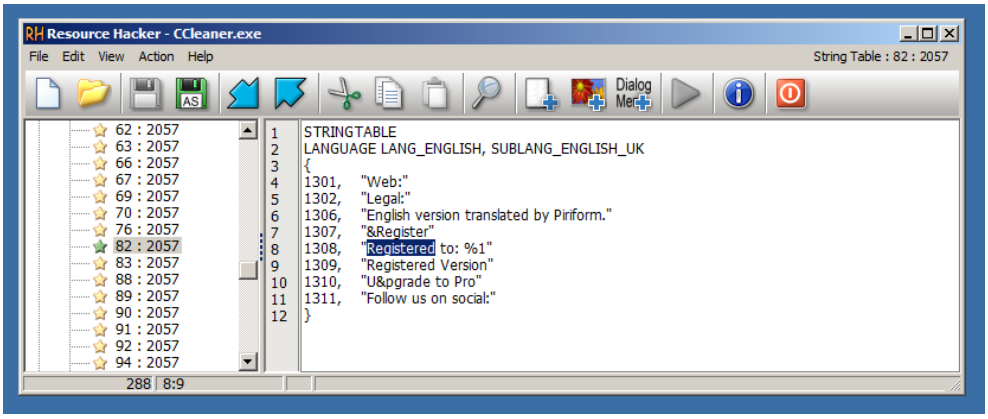
Al Ataque

Lo primero que debemos hacer es recolectar información del software, como en que lenguaje se desarrolló, si se encuentra protegido o empaquetado.

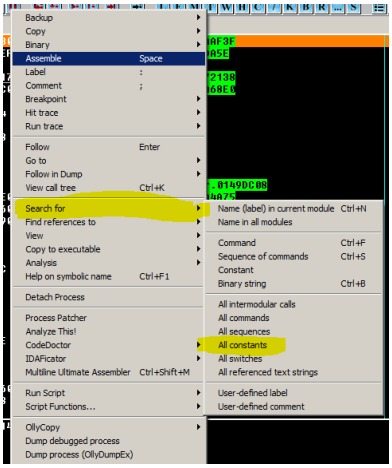
No muestra que el software fue desarrollado por Microsoft Visual C++ y que no está empaquetado, pero si está Protegido por IsDebuggerPresent, de lo cual una manera sencilla de evadir esta protección es cambiar su nombre de Ollydbg. XD



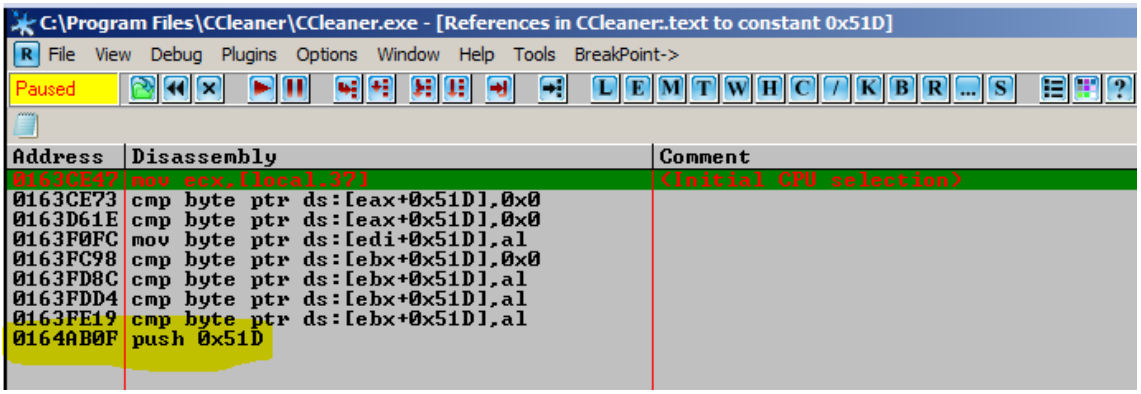
Luego usaremos Resource Hacker para poder encontrar la constante en donde se ubica el String “Registered Version”.



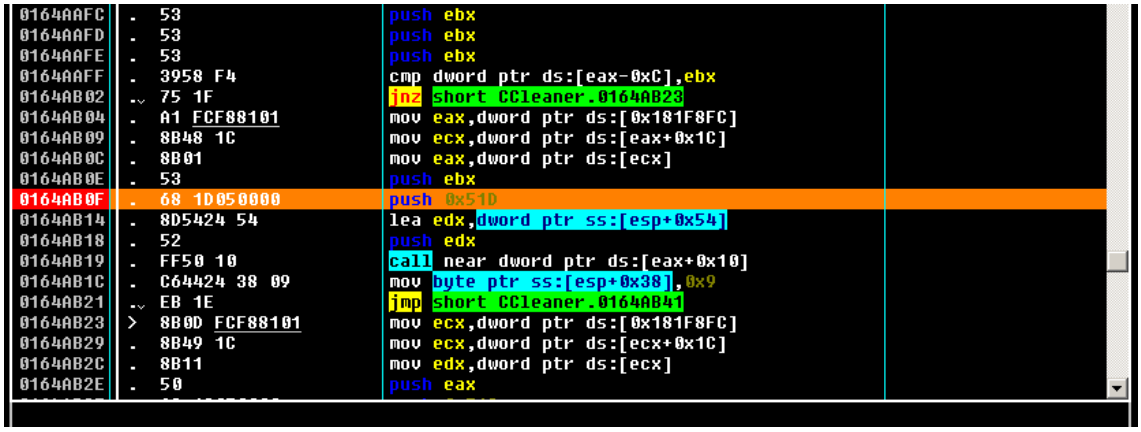
Abrimos Ollydbg, y buscamos todas las Constantes que tiene 1309.



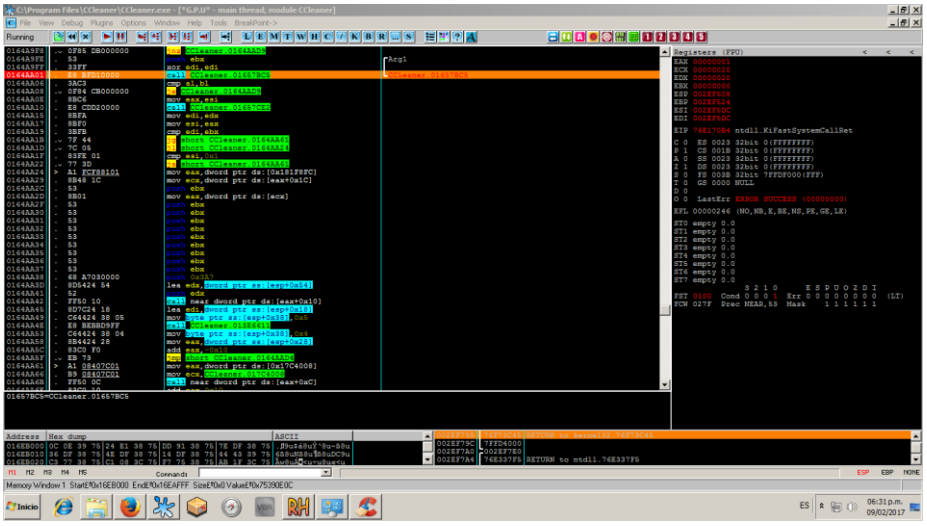
Seleccionamos la ultima linea PUSH. Hagamos doble click.



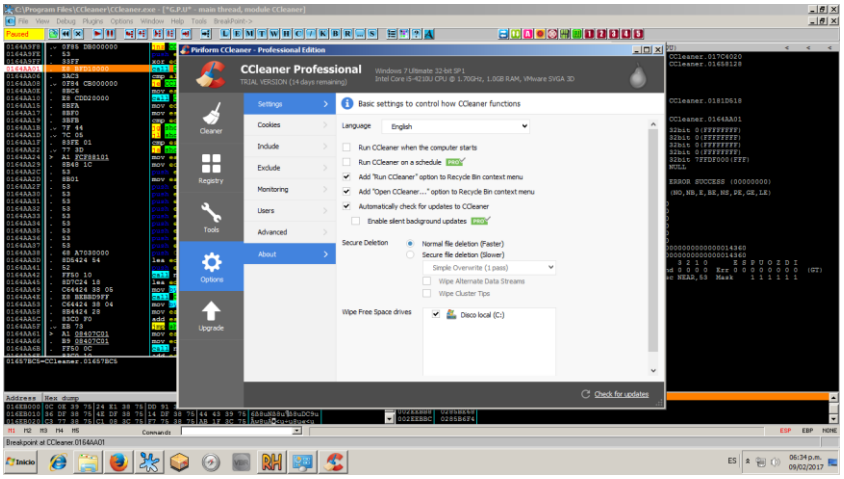
Al llegar en el area del Codigo, vemos que se ejecuta PUSH en donde si se registra nos muestra Registered Version (Version Registrado).



Para ello debemos ir mas arriba para poder ver en que punto se ejecuta el salto de bad boy. Para ellos debemos ir primero en el primer Argumento, en donde veras un Call, ahí agregamos un BreakPoint, y luego F9 (PLAY)



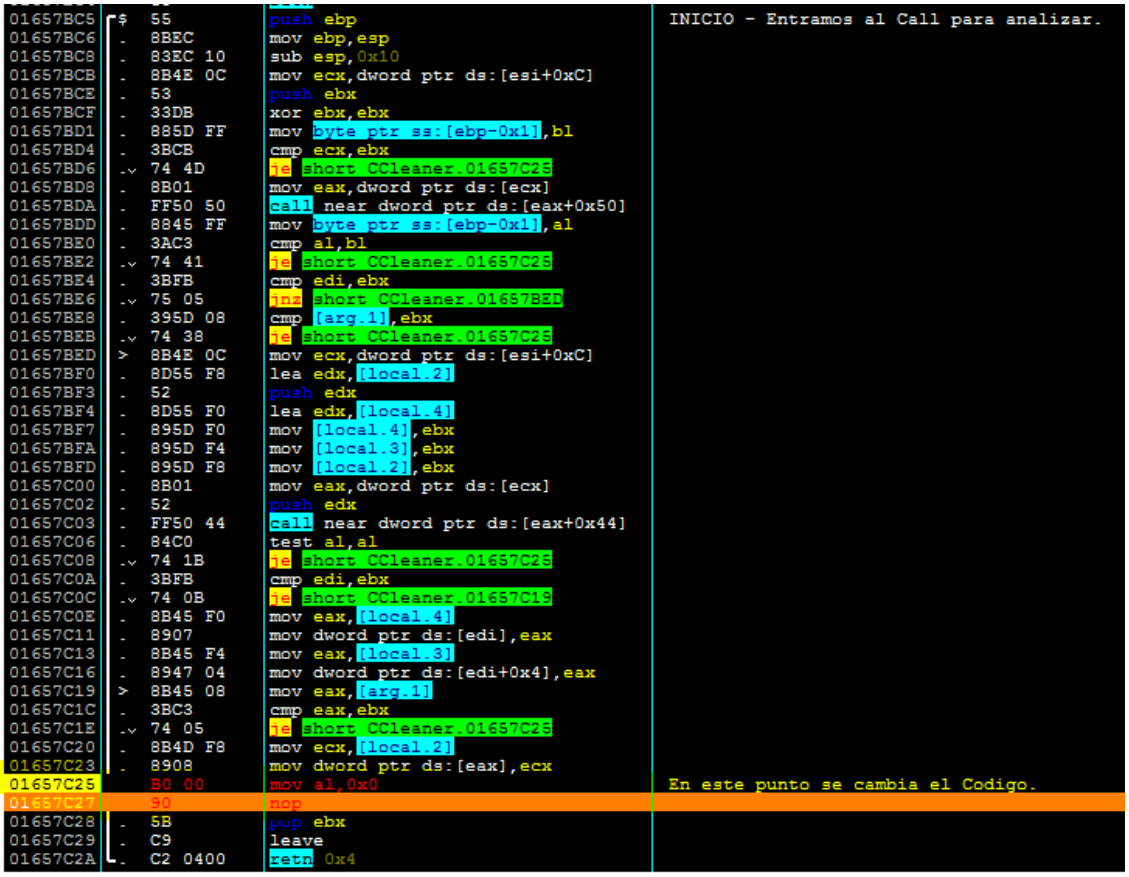
Cuando se ejecuta Ccleaner, vayamos a la opcion About, en donde veras que se detiene.



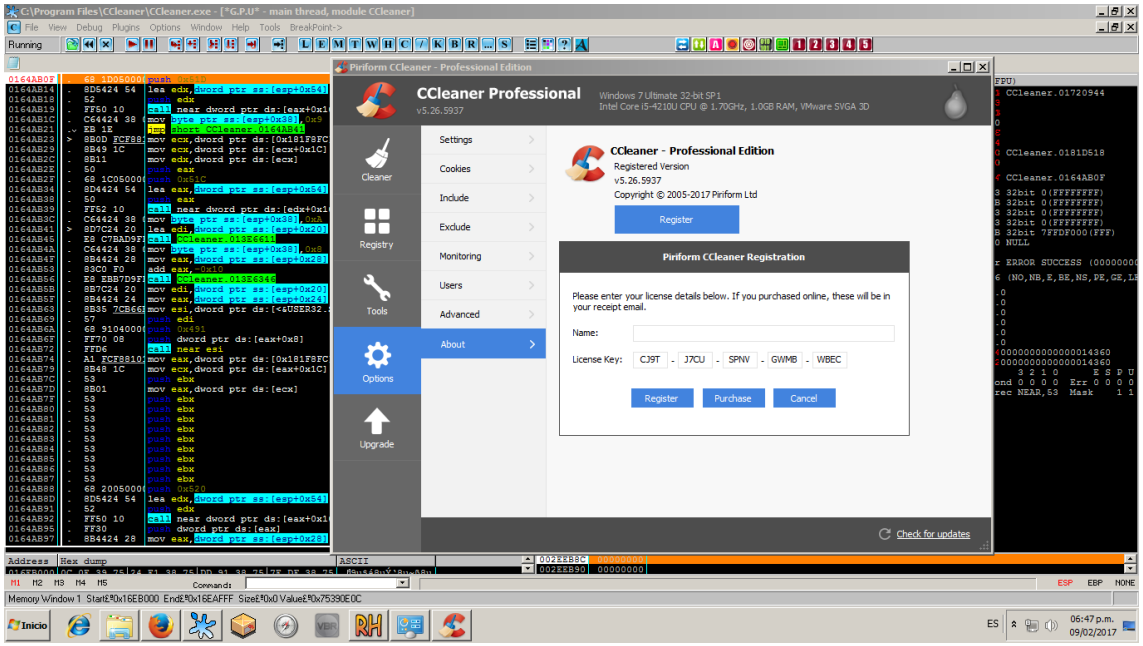
Vamos a tracear el CALL con la tecla F7.

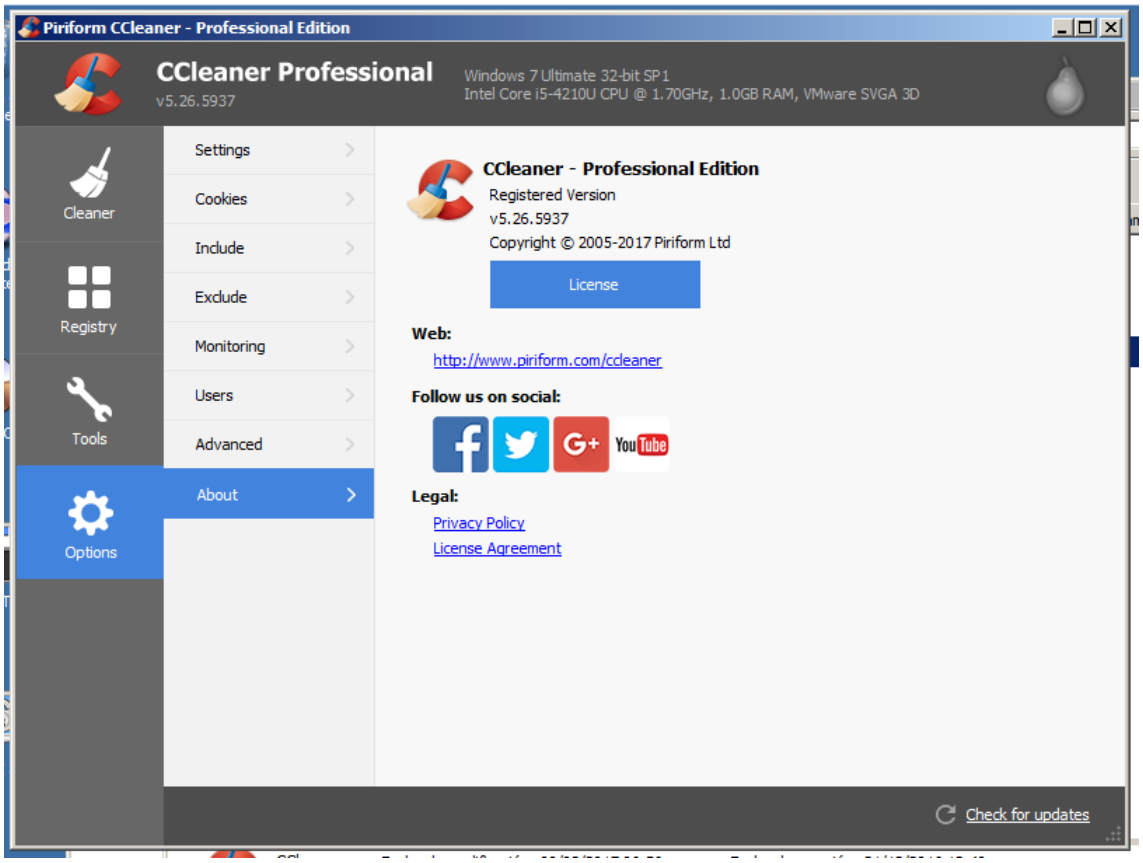
```
01657BC5  r$  55          push ebp                        INICIO - Entramos al Call para analizar.
01657BC6  .   8BEC        mov ebp,esp
01657BC8  .   83EC 10     sub esp,0x10
01657BCB  .   8B4E 0C     mov ecx,dword ptr ds:[esi+0xC]
01657BCE  .   53          push ebx
01657BCF  .   33DB        xor ebx,ebx
01657BD1  .   885D FF     mov byte ptr ss:[ebp-0x1],bl
01657BD4  .   3BCB        cmp ecx,ebx
01657BD6  .v  74 4D       je short CCleaner.01657C25
01657BD8  .   8B01        mov eax,dword ptr ds:[ecx]
01657BDA  .   FF50 50     call near dword ptr ds:[eax+0x50]
01657BDD  .   8845 FF     mov byte ptr ss:[ebp-0x1],al
01657BE0  .   3AC3        cmp al,bl
01657BE2  .v  74 41       je short CCleaner.01657C25
01657BE4  .   3BFB        cmp edi,ebx
01657BE6  .v  75 05       jnz short CCleaner.01657BED
01657BE8  .   395D 08     cmp [arg.1],ebx
01657BEB  .v  74 38       je short CCleaner.01657C25
01657BED  >   8B4E 0C     mov ecx,dword ptr ds:[esi+0xC]
01657BF0  .   8D55 F8     lea edx,[local.2]
01657BF3  .   52          push edx
01657BF4  .   8D55 F0     lea edx,[local.4]
01657BF7  .   895D F0     mov [local.4],ebx
01657BFA  .   895D F4     mov [local.3],ebx
01657BFD  .   895D F8     mov [local.2],ebx
01657C00  .   8B01        mov eax,dword ptr ds:[ecx]
01657C02  .   52          push edx
01657C03  .   FF50 44     call near dword ptr ds:[eax+0x44]
01657C06  .   84C0        test al,al
01657C08  .v  74 1B       je short CCleaner.01657C25
01657C0A  .   3BFB        cmp edi,ebx
01657C0C  .v  74 0B       je short CCleaner.01657C19
01657C0E  .   8B45 F0     mov eax,[local.4]
01657C11  .   8907        mov dword ptr ds:[edi],eax
01657C13  .   8B45 F4     mov eax,[local.3]
01657C16  .   8947 04     mov dword ptr ds:[edi+0x4],eax
01657C19  >   8B45 08     mov eax,[arg.1]
01657C1C  .   3BC3        cmp eax,ebx
01657C1E  .v  74 05       je short CCleaner.01657C25
01657C20  .   8B4D F8     mov ecx,[local.2]
01657C23  .   8908        mov dword ptr ds:[eax],ecx
01657C25  >   8A45 FF     mov al,byte ptr ss:[ebp-0x1]    En este punto se cambia el Codigo.
01657C28  .   5B          pop ebx
01657C29  .   C9          leave
01657C2A  L.  C2 0400     retn 0x4
01657C2D  >   8B48 0C     mov ecx,dword ptr ds:[eax+0xC]
```

Se modifco una linea para que el registro AL, tenga el valor 0 y asi salte a la ventana buena.



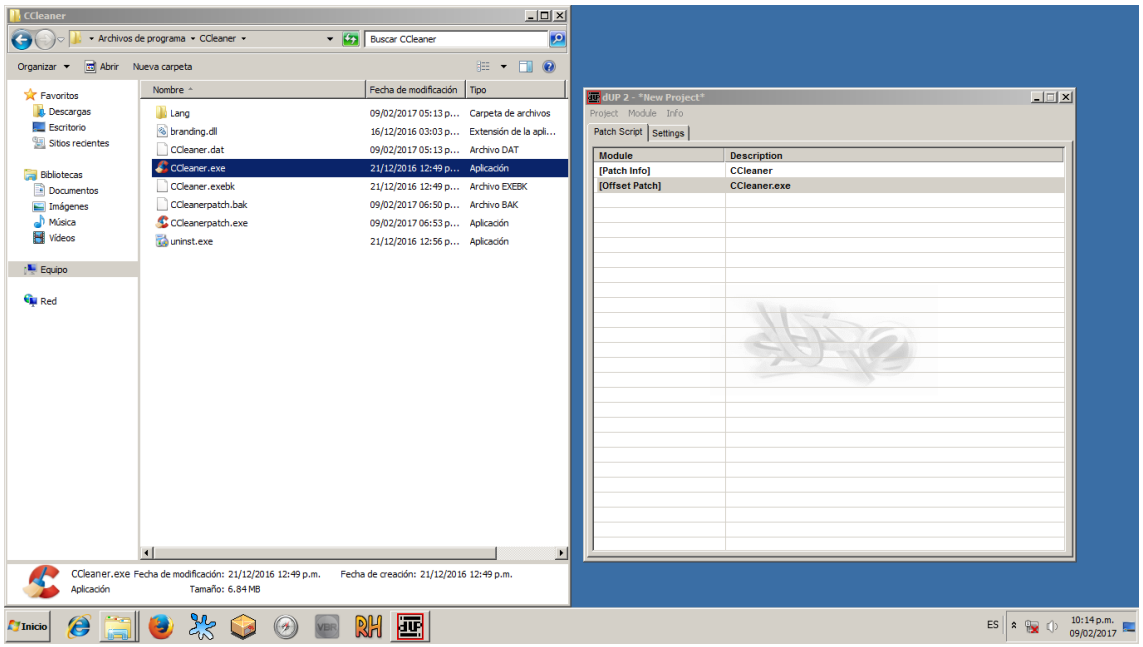
Y finalmente damos PLAY y validamos que nuestro Ccleaner este registrado



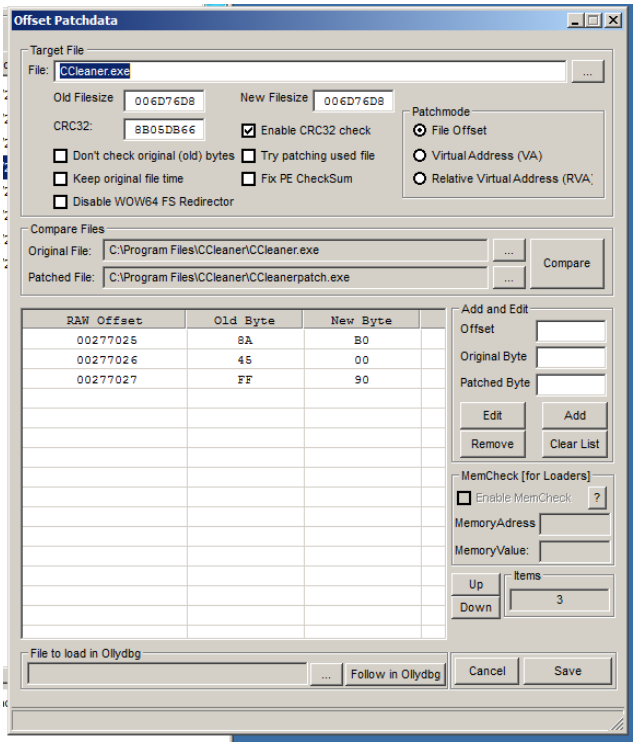


Herramienta DUP

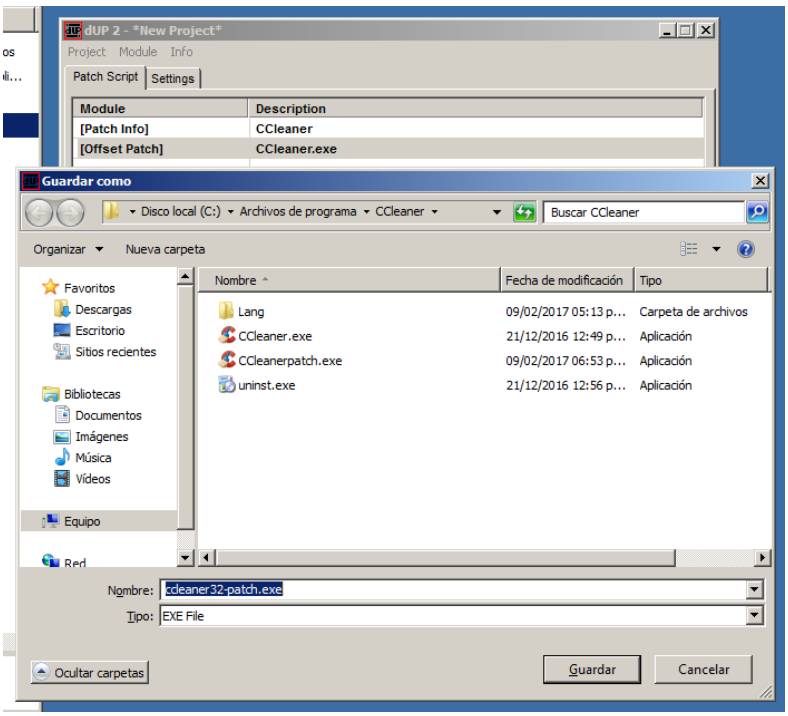
La Herramienta DUP, se utililiza para generar parches entre el archivo origina y el parchado. En este caso se utilizara para el Ccleaner de 32 bits.



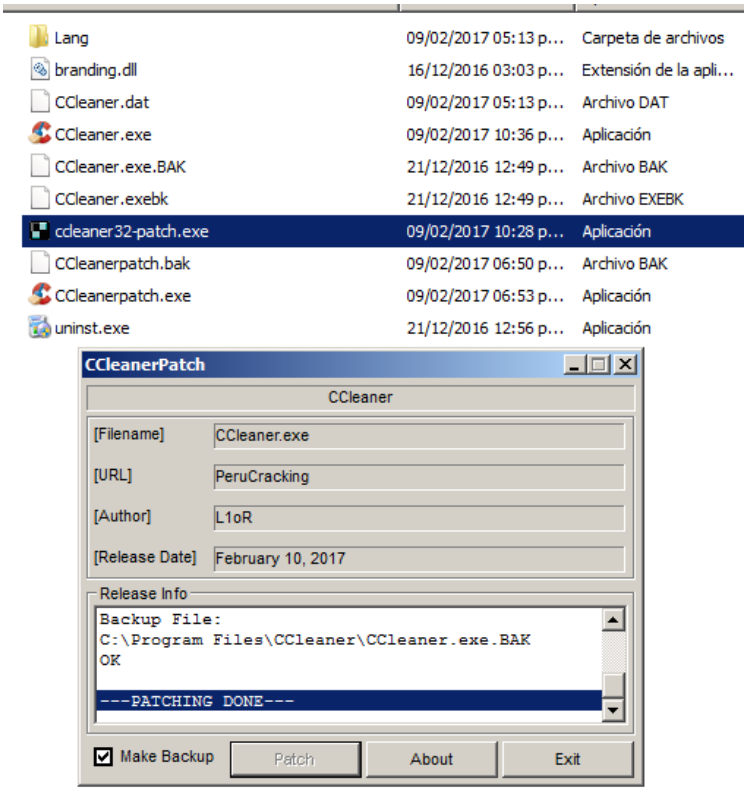
En este caso los bytes que se cambiaron fueron tres.



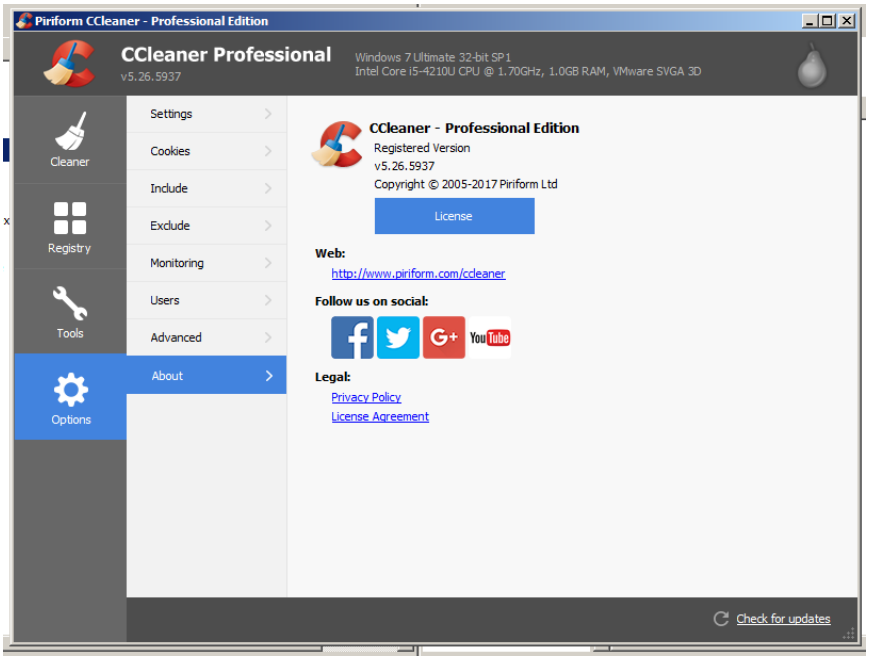
El patch lo puede guardar en el escritorio.



Copiamos nuestros Patch en la ruta donde se instalo el Ccleaner, y luego ejecutalo como Administrador, para que pueda parcharlo.


Lang 09/02/2017 05:13 p... Carpeta de archivos
branding.dll 16/12/2016 03:03 p... Extensión de la apli...
CCleaner.dat 09/02/2017 05:13 p... Archivo DAT
CCleaner.exe 09/02/2017 10:36 p... Aplicación
CCleaner.exe.BAK 21/12/2016 12:49 p... Archivo BAK
CCleaner.exebk 21/12/2016 12:49 p... Archivo EXEBK
ccleaner32-patch.exe 09/02/2017 10:28 p... Aplicación
CCleanerpatch.bak 09/02/2017 06:50 p... Archivo BAK
CCleanerpatch.exe 09/02/2017 06:53 p... Aplicación
uninst.exe 21/12/2016 12:56 p... Aplicación
CCleanerPatch
CCleaner
[Filename] CCleaner.exe
[URL] PeruCracking
[Author] L1oR
[Release Date] February 10, 2017
Release Info
Backup File:
C:\Program Files\CCleaner\CCleaner.exe.BAK
OK
---PATCHING DONE---
Make Backup
Patch
About
Exit

Finalmente :


Piriform CCleaner - Professional Edition
CCleaner Professional
v5.26.5937
Windows 7 Ultimate 32-bit SP1
Intel Core i5-4210U CPU @ 1.70GHz, 1.0GB RAM, VMware SVGA 3D
Cleaner
Registry
Tools
Options
Settings
Cookies
Include
Exclude
Monitoring
Users
Advanced
About
CCleaner - Professional Edition
Registered Version
v5.26.5937
Copyright © 2005-2017 Piriform Ltd
License
Web:
http://www.piriform.com/ccleaner
Follow us on social:
Legal:
Privacy Policy
License Agreement
Check for updates