CaptureWiz

[Escriba el subtítulo del documento]

Buscando registrarnos

13/12/2016

Programa	CaptureWiz (Pro) / (Lite)
Protección	Serial
Descarga	**http://pixelmetrics.com/CapWizPro/Download.htm** http://www.pixelmetrics.com/CapWizLite/Download.htm variada: http://pixelmetrics.com/Homepage/Downloads.htm
Descripción	Capturador de Pantalla
Herramienta	Ollydbg+ Tiempo
Objetivo	Registrarnos

Introducción

Bueno aquí estamos nuevamente con otro programita esta vez revisando que tanto logramos, esta vez el reto es ascendente, de una versión de referencia 2, llegar a la 6 que es la actual…veamos primero la actual y luego tomamos todas las versiones pilladas.

Se me ocurrió leer un tutorial de +NCR según el referia era el primer programa que reversaba

https://web.archive.org/web/20120211103653/http://www.reversinglabs.com.ar/ncr/tutoriales/01-capwizpro_+NCR.rar

me animé a ver que tanto lograba, terminaba de leer que habían 2 seriales validas

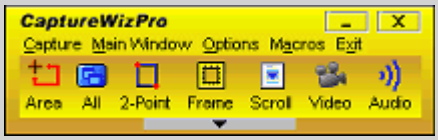
, este programa en una versión 2.x actualmente está en la versión 6 pero también es posible descargar las versiones anteriores: en el sitio

Old versions

CaptureWizPro 5.4

CaptureWizPro 4.5

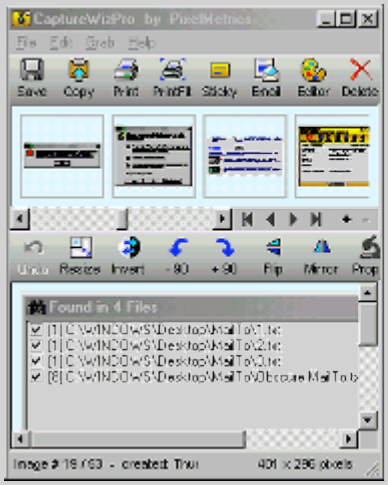
CaptureWizPro 3.B



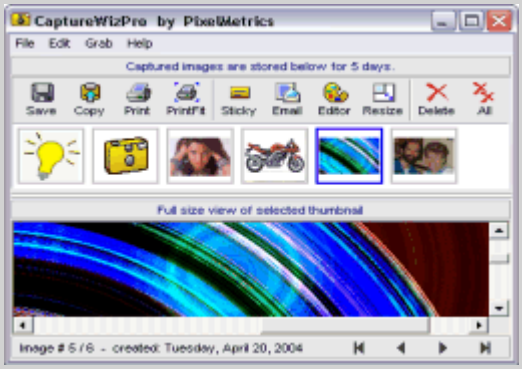
CaptureWizPro 3.A Same appearance as 3.B above

CaptureWizPro 3.6 Same appearance as 3.B above

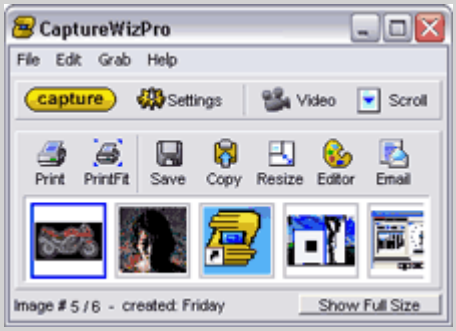
CaptureWizPro 3.2



CaptureWizPro 3.1

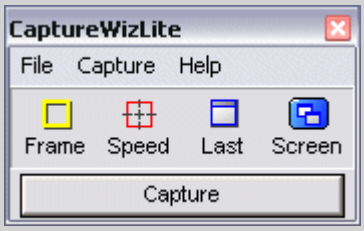


CaptureWizPro 2.3

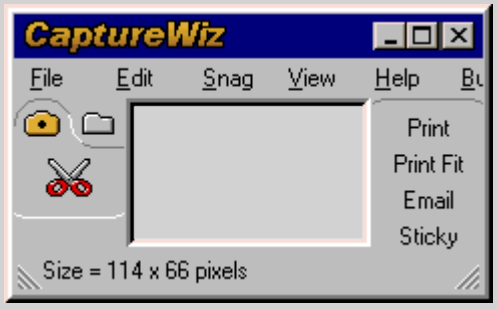


CaptureWizPro 1.32

CaptureWiz **Lite** 2.4



CaptureWiz 1.11

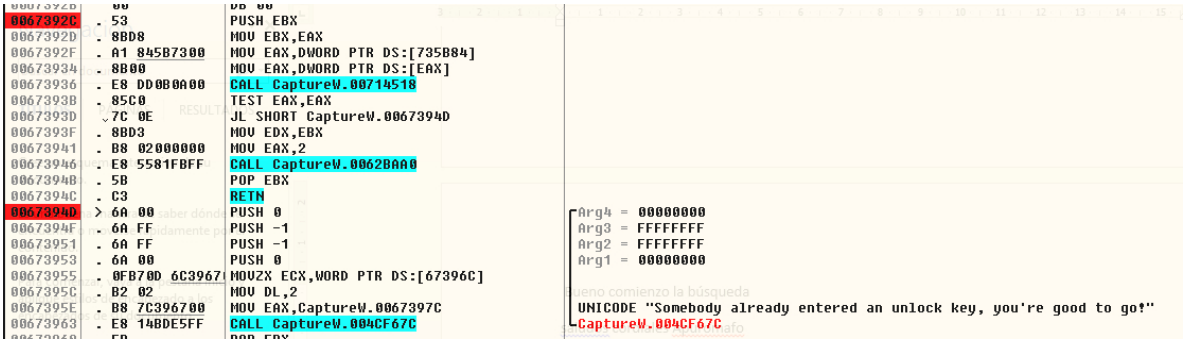


Oldest available - Jan 2001

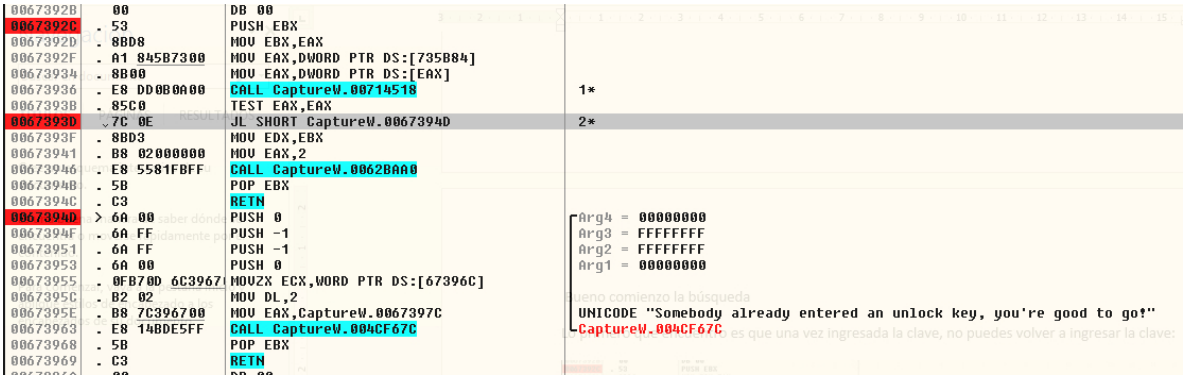
Replaced by CaptureWizLite, but still available. CaptureWizLite accepts this program's keys.

Bueno comienzo la búsqueda en la versión nueva 6.10

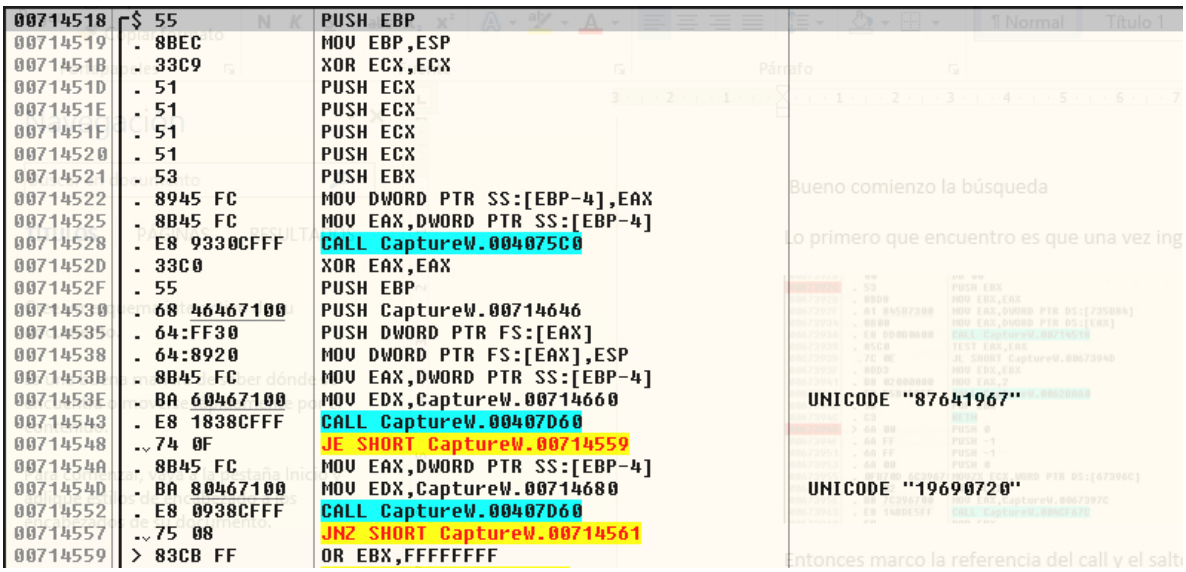
Lo primero que encuentro es que una vez ingresada la clave, no puedes volver a ingresar la clave(está en inglés):



Entonces marco la referencia del call y el salto



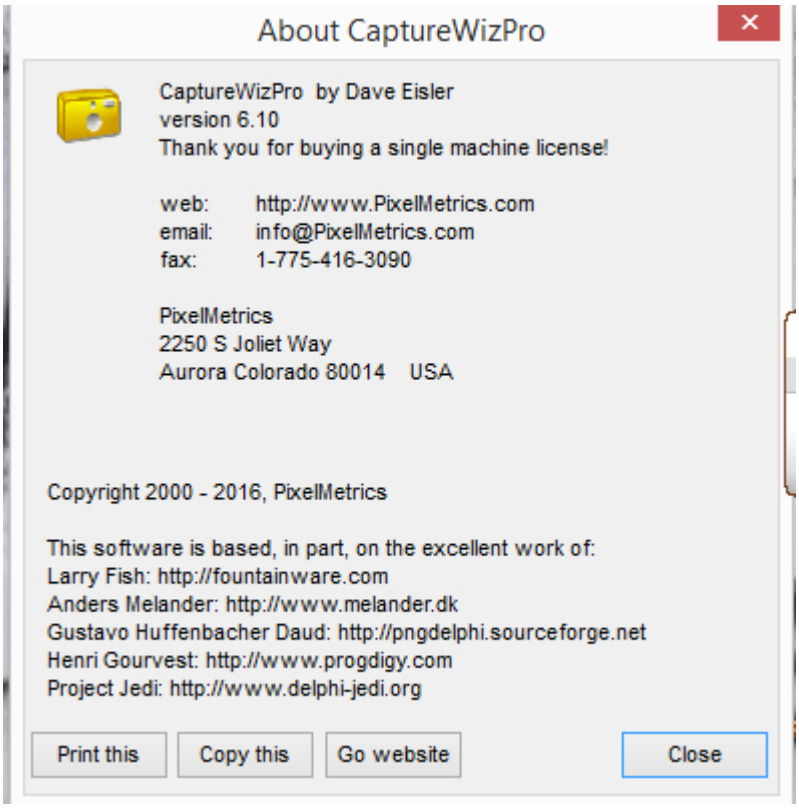
Al entrar al call encuentro 2 valores



No quiero pensar mal…pero es asi

Al ingresar cualquiera de los 2 seriales se registra, y si anulo el salto con nop, puedo volver a ingresar la licencia a otra..pero ya está activado.

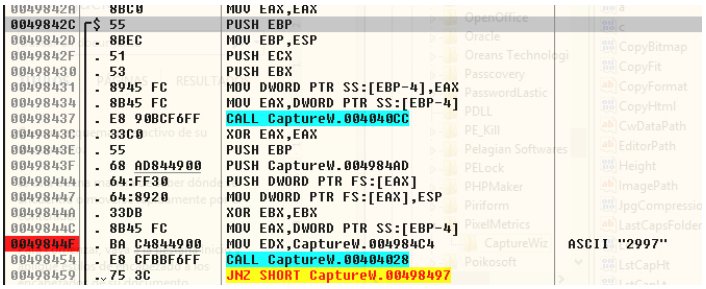
Antes de la llamada hay algunos call, y antes de eso el llamado de gracias por registrar.



Aprovechando que están disponibles más versiones veamos uno a uno y así evito hacer varios tutoriales para el mismo programa

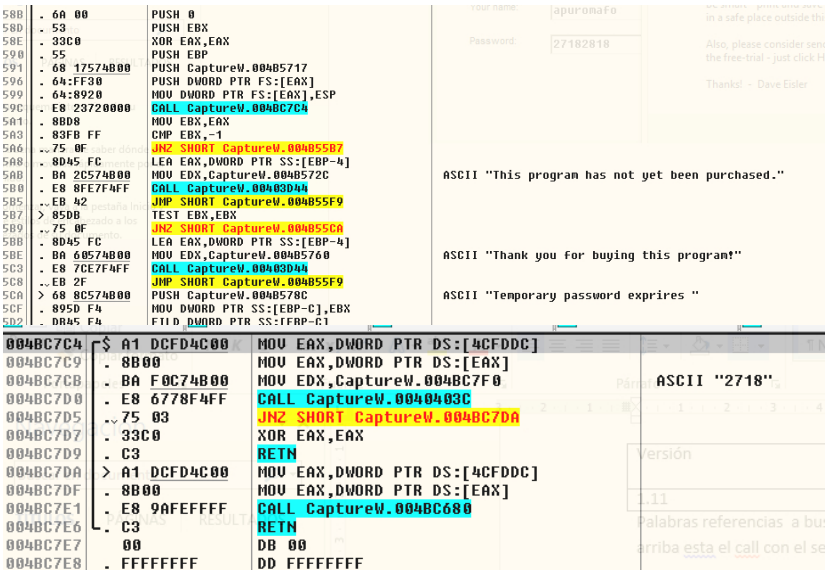
Versión	Nombre(cualquiera) Serial:
1.11	2997

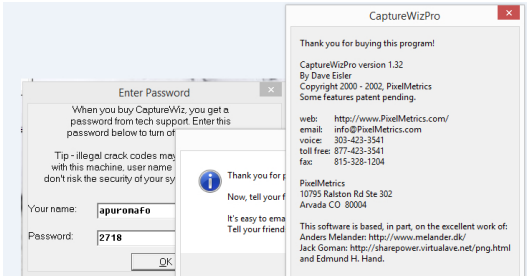
Palabras referencias a buscar “Buy” que hace alusión a gracias por registrar..un salto mas arriba esta el call con el serial valido



Versión	Nombre(cualquiera) Serial:
1.32	2718

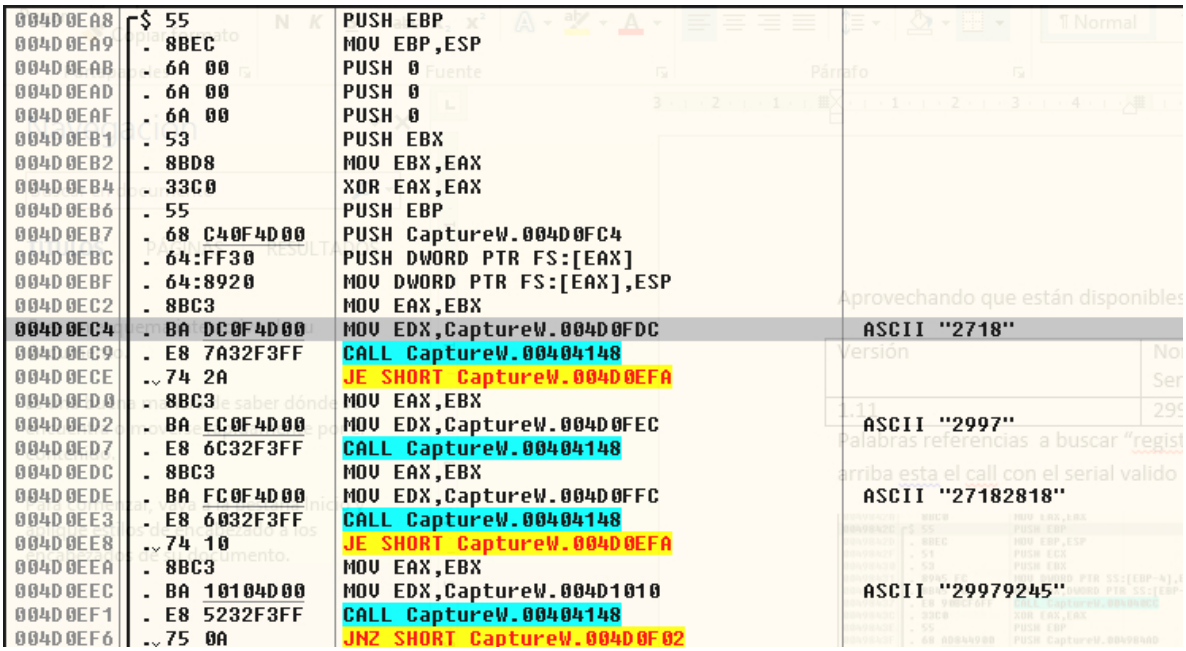
Palabras referencias a buscar “Buying” que hace alusión a gracias por registrar..un salto mas arriba esta el call con el serial valido





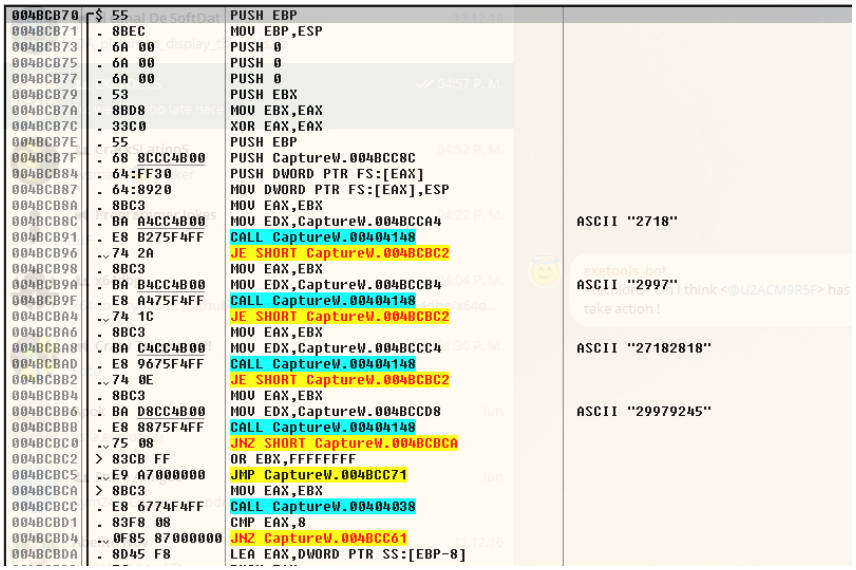
Versión	Nombre(cualquiera) Serial:
2.3	27182818

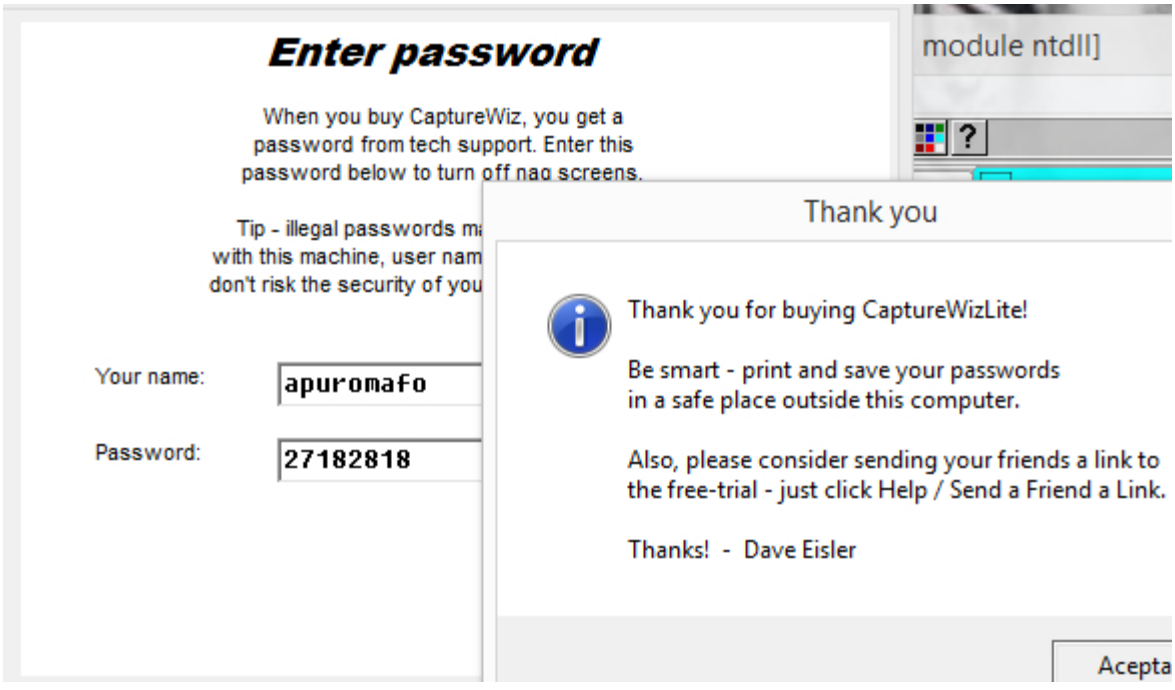
Igual hay mas aquí lo pueden apreciar el serial son 4 validos



Versión	Nombre(cualquiera) Serial:
2.4 Lite	27182818

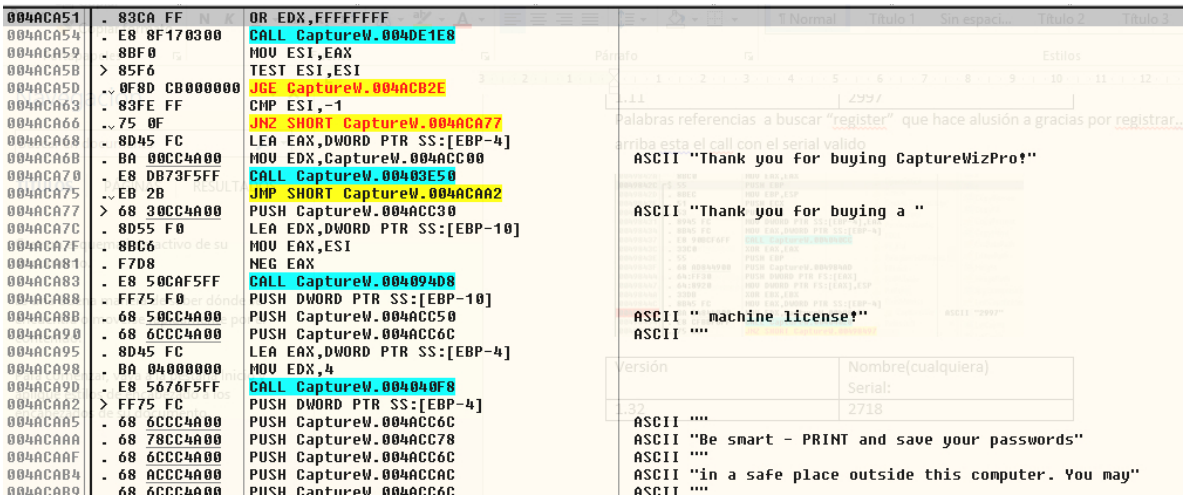
De nuevo 4 seriales



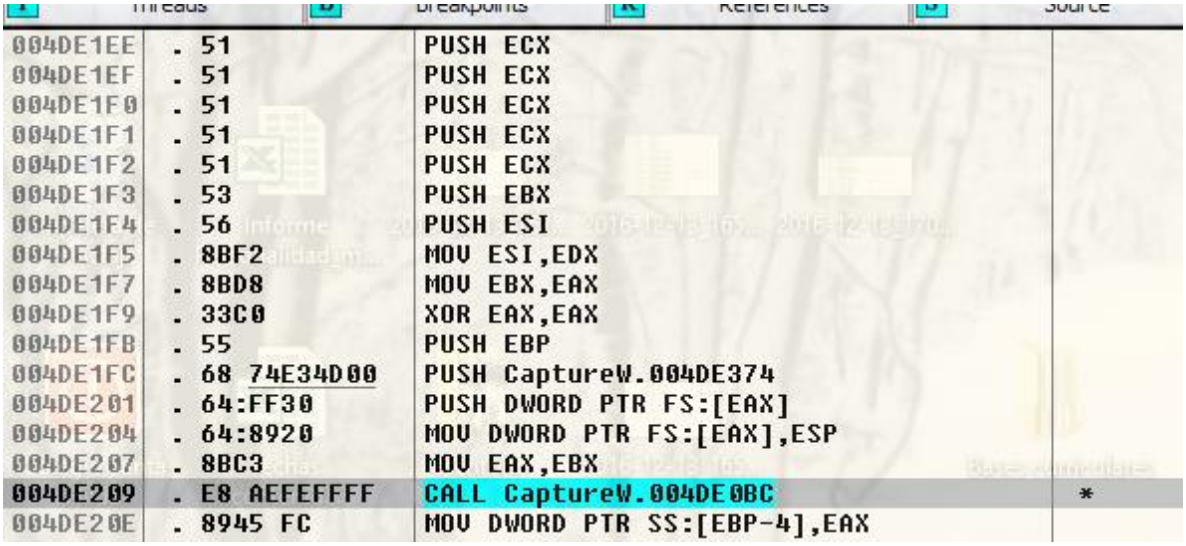


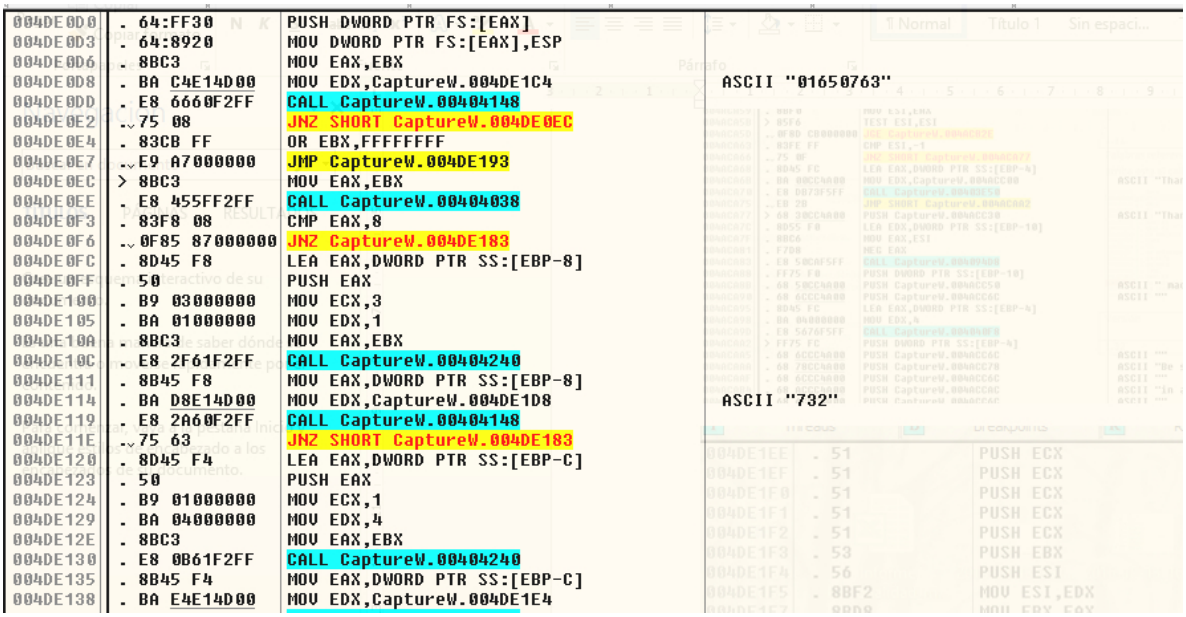
Versión	Nombre(cualquiera) Serial:
3.1	01650763

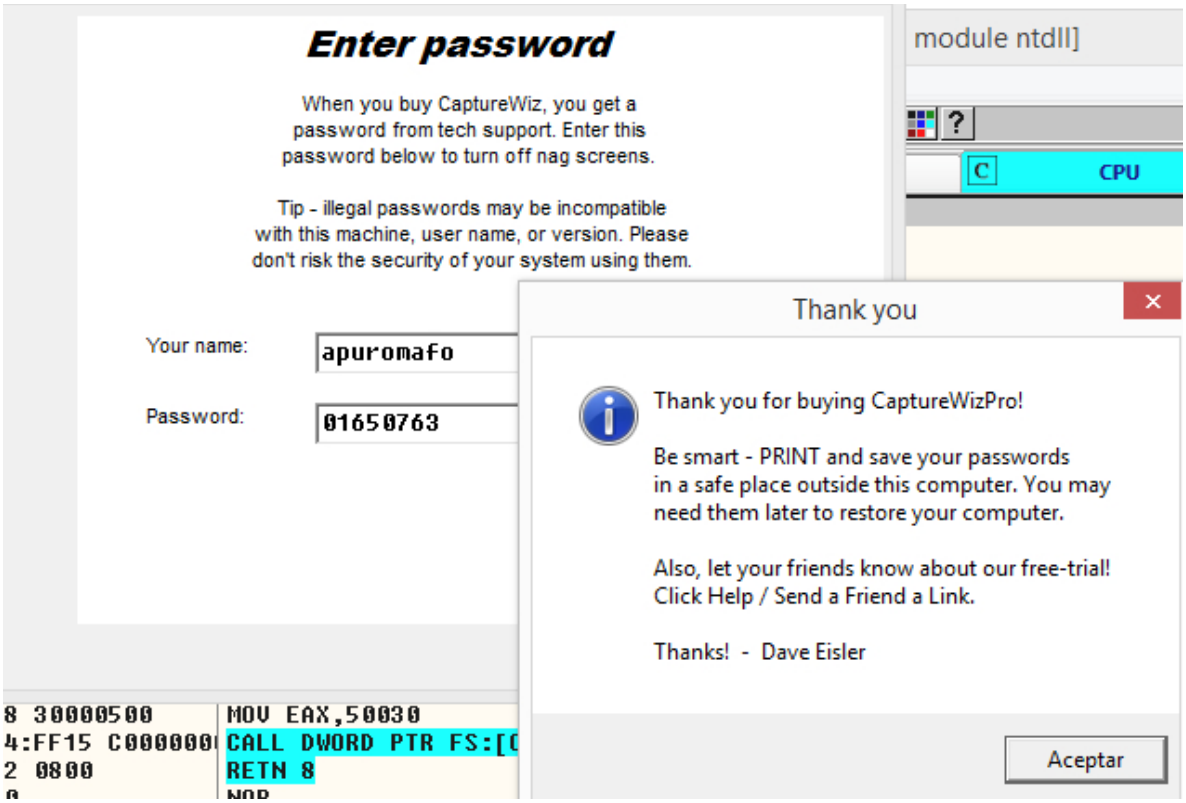
Aquí el mismo método, pero el call



Llama a otro call, claramente ya se ven mas validaciones

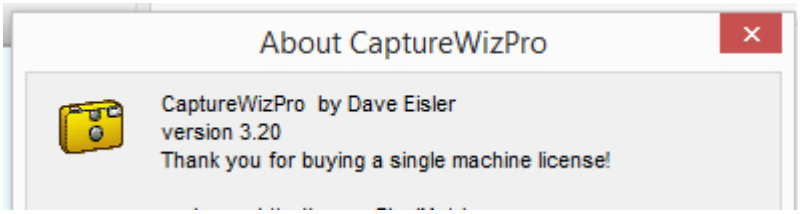


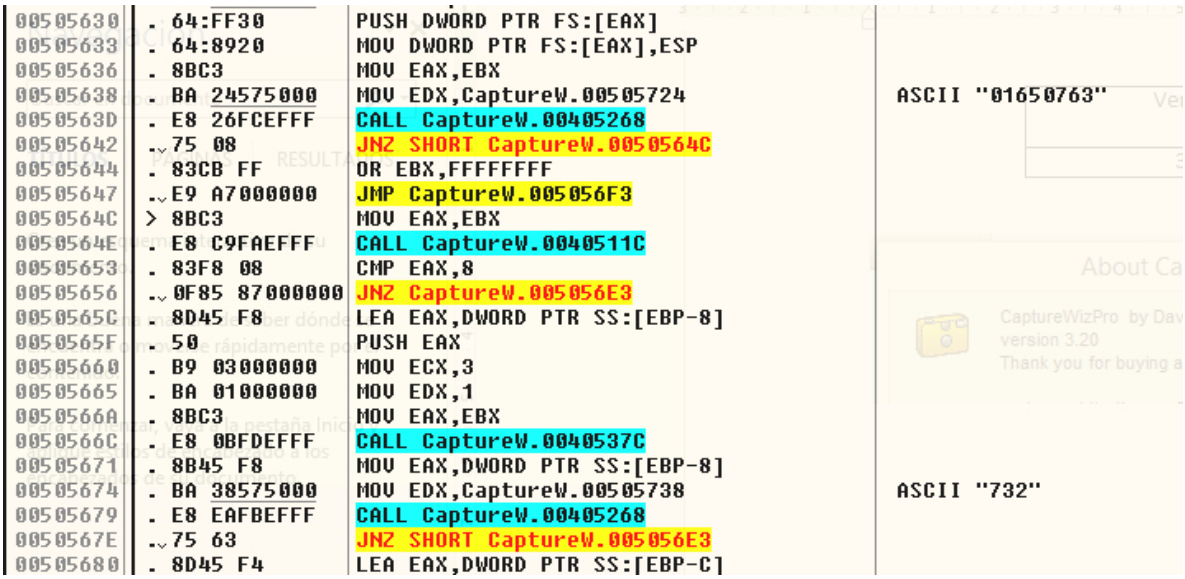

004DE0D0 . 64:FF30 PUSH DWORD PTR FS:[EAX]
004DE0D3 . 64:8920 MOV DWORD PTR FS:[EAX],ESP
004DE0D6 . 8BC3 MOV EAX,EBX
004DE0D8 . BA C4E14D00 MOV EDX,CaptureW.004DE1C4
004DE0DD . E8 6660F2FF CALL CaptureW.00404148
004DE0E2 . 75 08 JNZ SHORT CaptureW.004DE0EC
004DE0E4 . 83CB FF OR EBX,FFFFFFFF
004DE0E7 . E9 A7000000 JMP CaptureW.004DE193
004DE0EC > 8BC3 MOV EAX,EBX
004DE0EE . E8 455FF2FF CALL CaptureW.00404038
004DE0F3 . 83F8 08 CMP EAX,8
004DE0F6 . 0F85 87000000 JNZ CaptureW.004DE183
004DE0FC . 8D45 F8 LEA EAX,DWORD PTR SS:[EBP-8]
004DE0FF . 50 PUSH EAX
004DE100 . B9 03000000 MOV ECX,3
004DE105 . BA 01000000 MOV EDX,1
004DE10A . 8BC3 MOV EAX,EBX
004DE10C . E8 2F61F2FF CALL CaptureW.00404240
004DE111 . 8B45 F8 MOV EAX,DWORD PTR SS:[EBP-8]
004DE114 . BA D8E14D00 MOV EDX,CaptureW.004DE1D8
004DE119 . E8 2A60F2FF CALL CaptureW.00404148
004DE11E . 75 63 JNZ SHORT CaptureW.004DE183
004DE120 . 8D45 F4 LEA EAX,DWORD PTR SS:[EBP-C]
004DE123 . 50 PUSH EAX
004DE124 . B9 01000000 MOV ECX,1
004DE129 . BA 04000000 MOV EDX,4
004DE12E . 8BC3 MOV EAX,EBX
004DE130 . E8 0B61F2FF CALL CaptureW.00404240
004DE135 . 8B45 F4 MOV EAX,DWORD PTR SS:[EBP-C]
004DE138 . BA E4E14D00 MOV EDX,CaptureW.004DE1E4
ASCII "01650763"
ASCII "732"


Enter password
When you buy CaptureWiz, you get a password from tech support. Enter this password below to turn off nag screens.
Tip - illegal passwords may be incompatible with this machine, user name, or version. Please don't risk the security of your system using them.
Your name:
apuromafo
Password:
01650763
module ntdll]
CPU
Thank you
Thank you for buying CaptureWizPro!
Be smart - PRINT and save your passwords in a safe place outside this computer. You may need them later to restore your computer.
Also, let your friends know about our free-trial! Click Help / Send a Friend a Link.
Thanks! - Dave Eisler
Aceptar
8 30000500 MOV EAX,50030
4:FF15 C000000 CALL DWORD PTR FS:[
2 0800 RETN 8

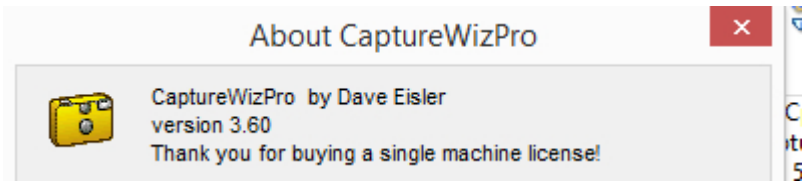
Versión	Nombre(cualquiera) Serial:
3.2	01650763

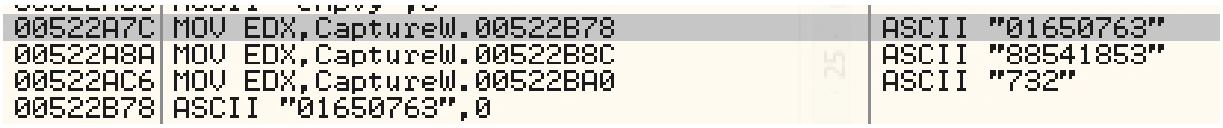
Ya el serial comienza a usarse en mas de una version



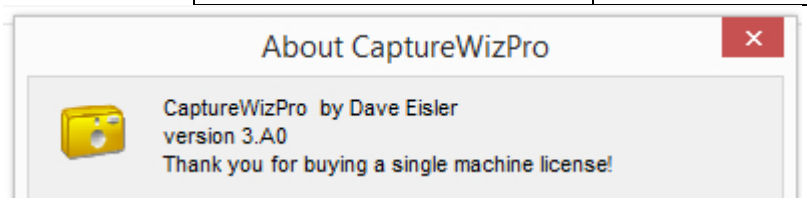


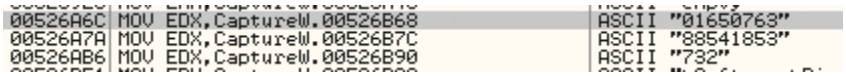
Versión	Nombre(cualquiera) Serial:
3.6	01650763



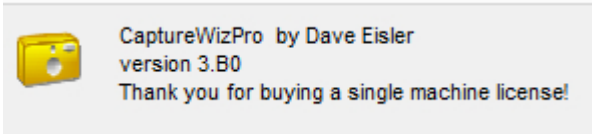


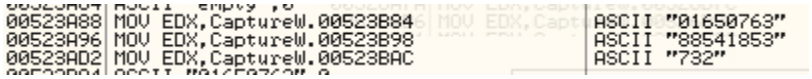
Versión	Nombre(cualquiera) Serial:
3.6A0	01650763





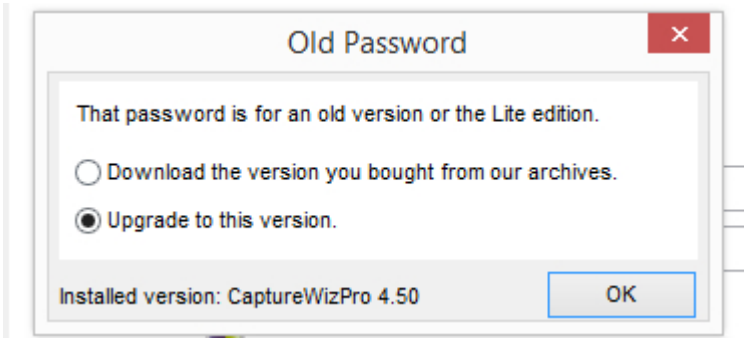
Versión	Nombre(cualquiera) Serial:
3.6A0	01650763

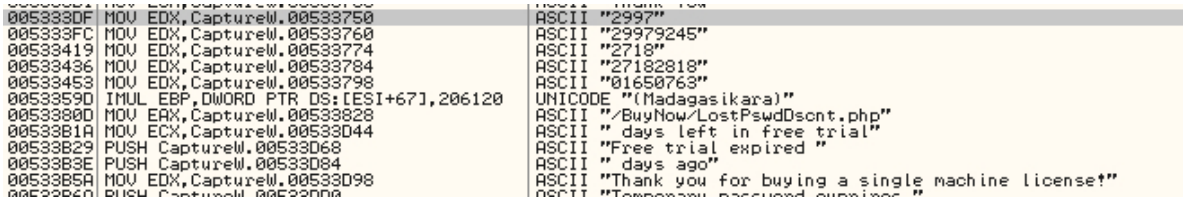




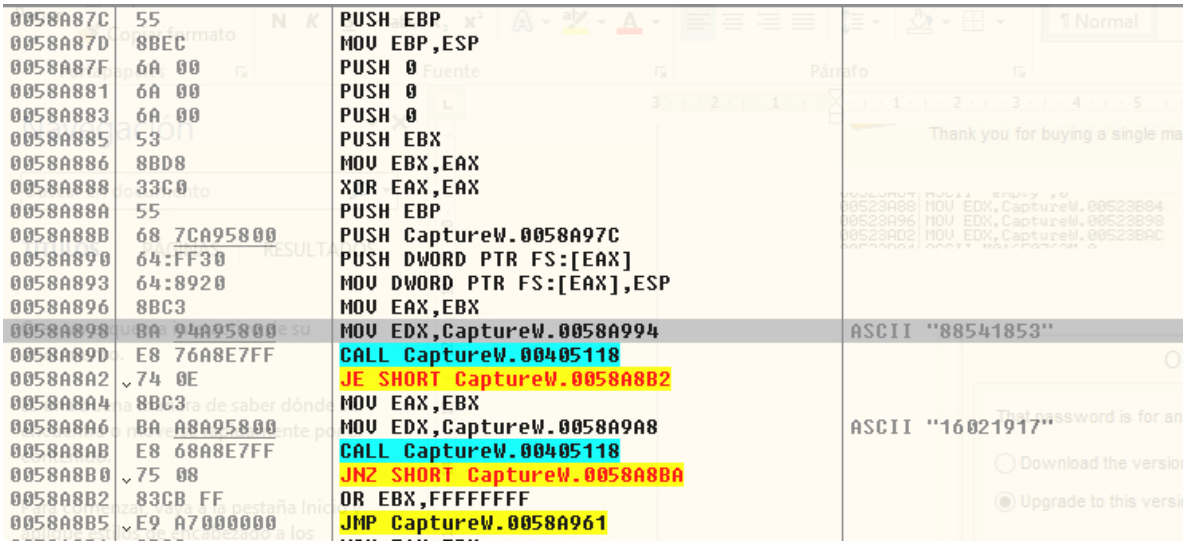
Versión	Nombre(cualquiera) Serial:
4.5	88541853

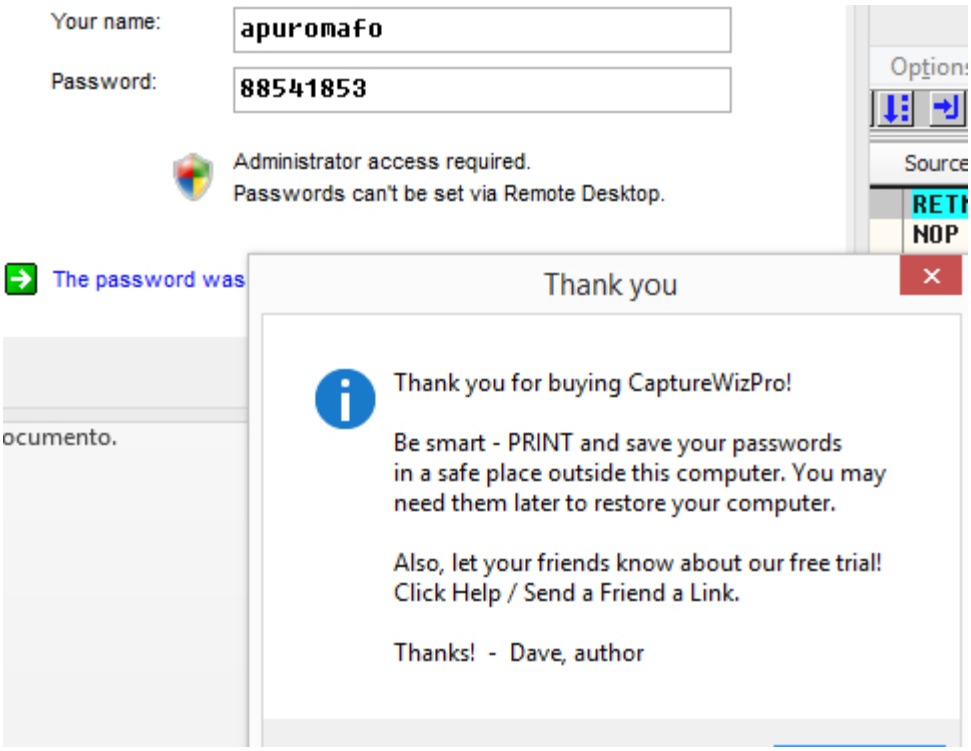
29979245, 27182818,2718,27182818,01650763 muestra:





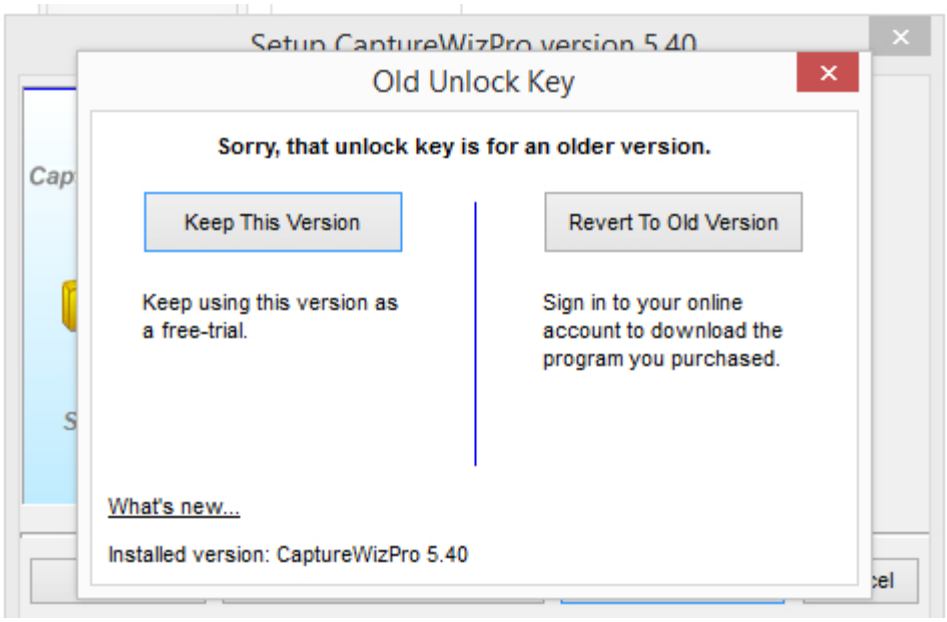
Ahora busco con las referencias nuevas con la misma estructura buy…luego buscar el primer call, entro y encuentro 88541853





Versión	Nombre(cualquiera) Serial:
4.5	88541853

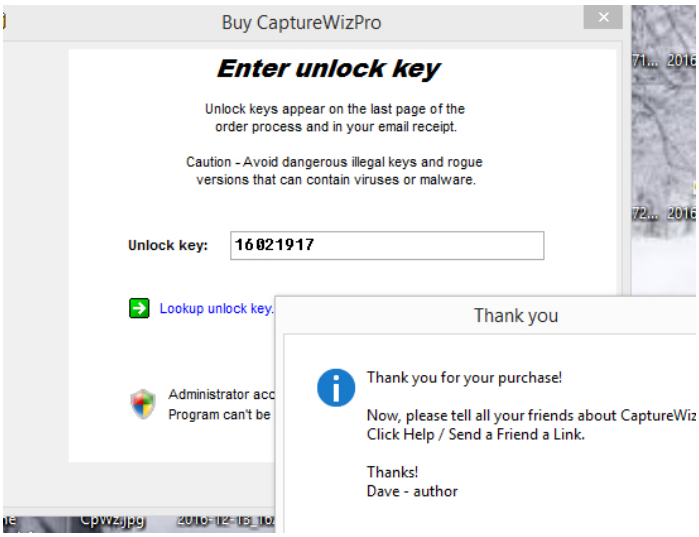
Con el serial anterior 88541853

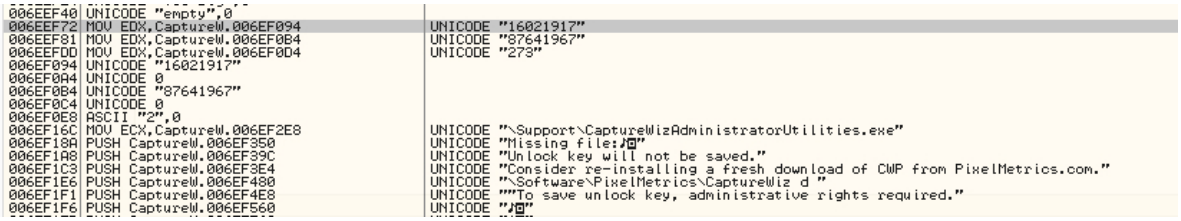



```
00631301 ASCII "Sender"
00631312 ASCII "TfrmPswdOld"
00631328 ASCII "PswdOld"
00631344 UNICODE "2997",0
0063135C UNICODE "29979245"
0063136C UNICODE 0
0063137C UNICODE "2718",0
00631394 UNICODE "27182818"
006313A4 UNICODE 0
006313B4 UNICODE "01650763"
006313C4 UNICODE 0
006313D4 UNICODE "88541853"
006313E4 UNICODE 0
00631462 MOV EDX,CaptureW.00631618
```

UNICODE "Instal

Probamos el segundo que no verificamos: 16021917



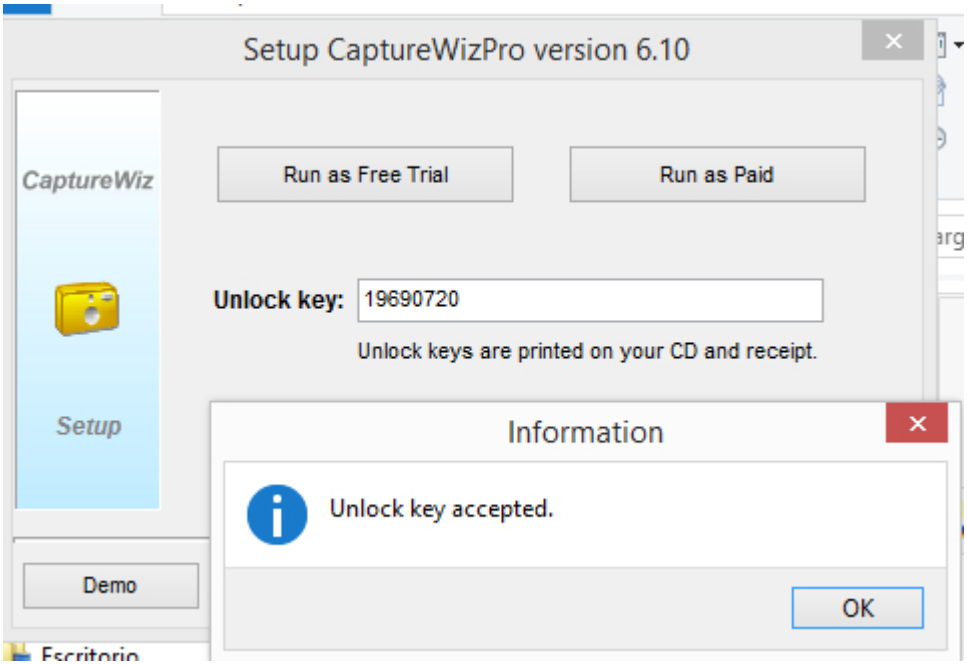


Y como hemos de suponer el segundo serial es para la próxima versión (19690720) si siguen al mismo ritmo

6.10	87641967, 19690720
Próxima?	19690720 o una nueva rama numérica

Con eso podemos comentar que a pesar del tutorial de +NCR el autor siguió escribiendo el mismo algoritmo de validación que guarda el serial base, algunas validaciones adicionales, pero el mismo algoritmo en si que solo compara con 2 seriales válidas.

Cabe destacar si algúno quiere un descuento, solo debe desinstalar y en algún caso random, aparece un link promocional



Bueno terminando con el tema el autor ha creado otros programas, algunos siguieron gracias a el capturador como versión free, otras sin soporte solo para quienes han comprado el programa

http://pixelmetrics.com/Consulting/Consulting.htm

un abrazo a la distancia Apuromafo

solo dejar un saludo a quien se ha dado el tiempo de leer este escrito ☺