

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](#)

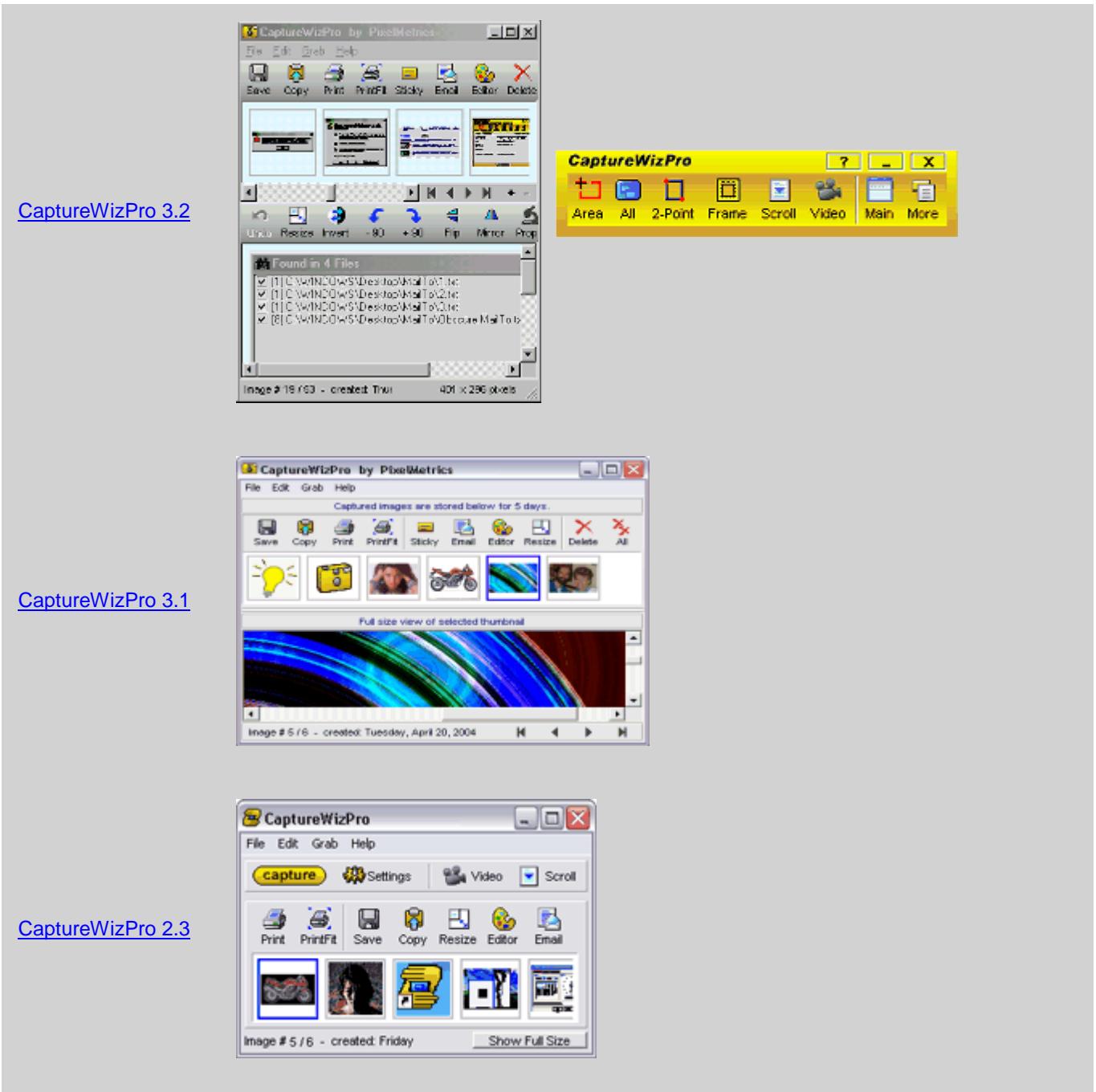


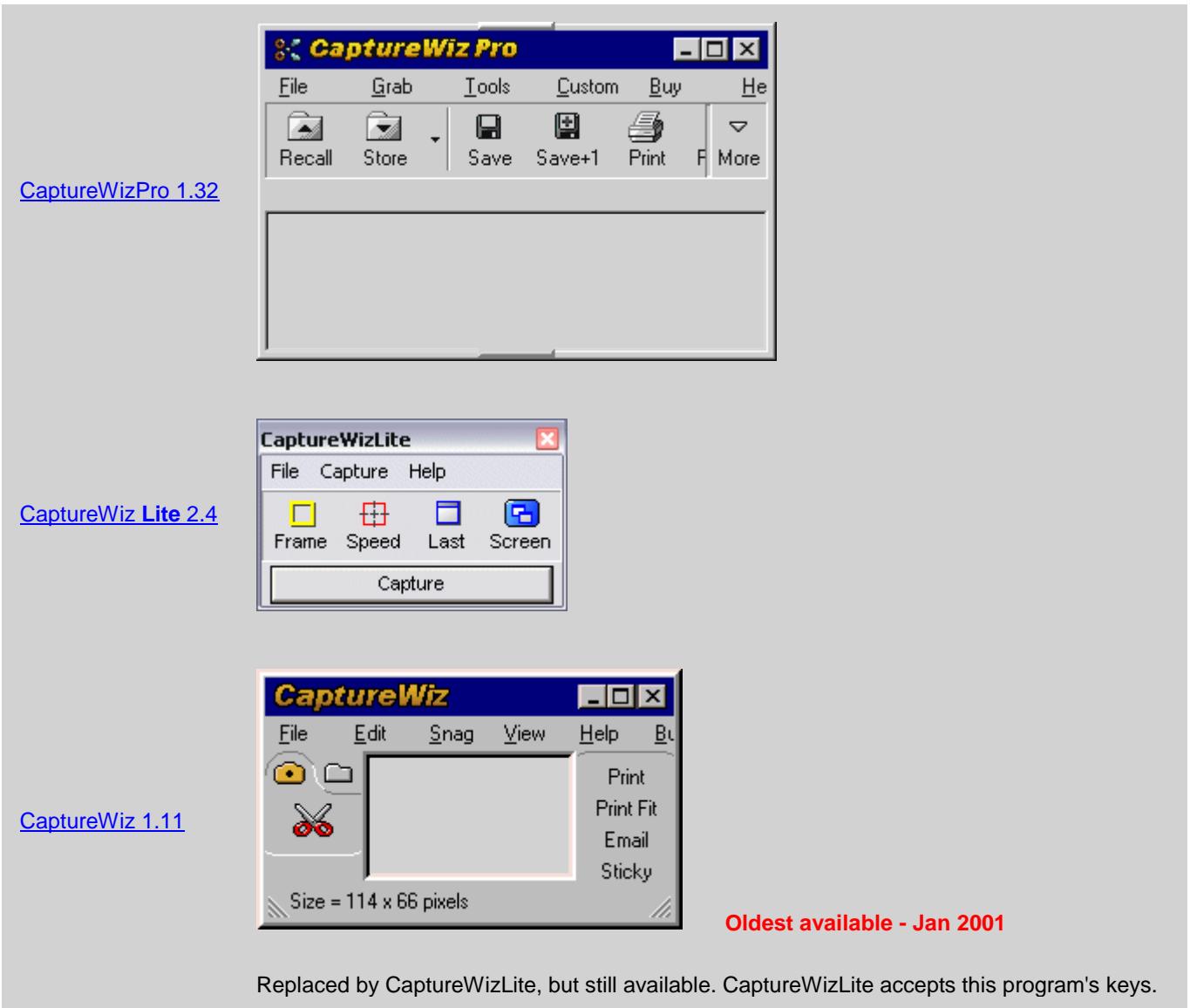
[CaptureWizPro 3.B](#)



[CaptureWizPro 3.A](#) Same appearance as 3.B above

[CaptureWizPro 3.6](#) Same appearance as 3.B above





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):

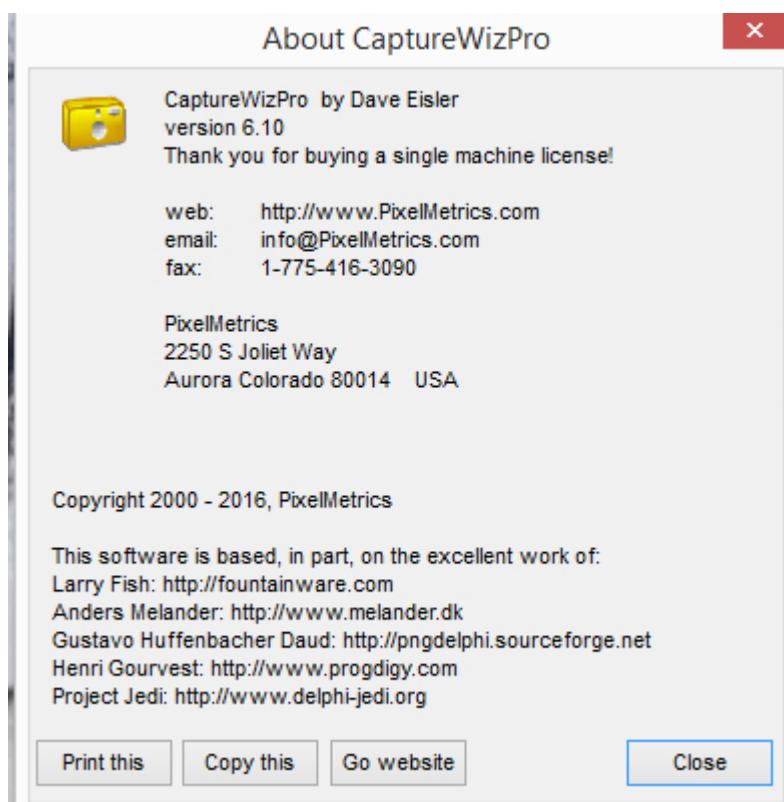
Entonces marco la referencia del call y el salto

Al entrar al call encuentro 2 valores

No quiero pensar mal...pero es así

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.



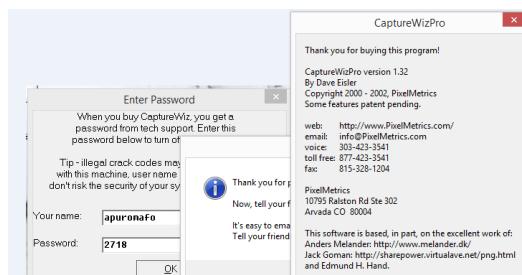
Aprovechando que están disponibles más versiones veamos uno a uno y así evito hacer varios tutoriales para el mismo programa

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

```

004D0EA8 $ 55          PUSH EBP
004D0EA9 . 8BEC        MOV EBP,ESP
004D0EAB . 6A 00        PUSH 0
004D0EAD . 6A 00        PUSH 0
004D0EAF . 6A 00        PUSH 0
004D0EB1 . 53          PUSH EBX
004D0EB2 . 8BD8        MOV EBX,EAX
004D0EB4 . 33C0        XOR EAX,EAX
004D0EB6 . 55          PUSH EBP
004D0EB7 . 68 C40F4D00  PUSH CaptureW.004D0FC4
004D0EBC . 64:FF30     PUSH DWORD PTR FS:[EAX]
004D0EBF . 64:8920     MOV DWORD PTR FS:[EAX],ESP
004D0EC2 . 8BC3        MOV EAX,EBX
004D0EC4 . BA DC0F4D00  MOV EDX,CaptureW.004D0FDC
004D0EC9 . E8 7A32F3FF  CALL CaptureW.004D04148
004D0ECE .~74 2A        JE SHORT CaptureW.004D0EFA
004D0ED0 . 8BC3        MOV EAX,EBX
004D0ED2 . BA EC0F4D00  MOV EDX,CaptureW.004D0FEC
004D0ED7 . E8 6C32F3FF  CALL CaptureW.004D04148
004D0EDC . 8BC3        MOV EAX,EBX
004D0EDE . BA FC0F4D00  MOV EDX,CaptureW.004D0FFC
004D0EE3 . E8 6032F3FF  CALL CaptureW.004D04148
004D0EE8 .~74 10        JE SHORT CaptureW.004D0EFA
004D0EEA . 8BC3        MOV EAX,EBX
004D0EEC . BA 10104D00  MOV EDX,CaptureW.004D1010
004D0EF1 . E8 5232F3FF  CALL CaptureW.004D04148
004D0EF6 .~75 0A        JNZ SHORT CaptureW.004D0F02

```

Aprovechando que están disponibles

ASCII "2718"

Versión No
Ser

1.11 ASCII "2997"

Palabras Referencias a buscar "regist
arriba esta el call con el serial valido

ASCII "27182818"

ASCII "29979245"

004D0EAD . 55 PUSH EBP
004D0EBC . 8BEC MOV EBP,ESP
004D0ECE .~54 2A PUSH EAX
004D0ED0 . 8BC3 MOV EBX,EAX
004D0ED7 . 8BEC MOV EBP,ESP
004D0EDC . 55 PUSH EBP
004D0EE3 . 8BEC MOV EBP,ESP
004D0EE8 .~54 10 PUSH EAX
004D0EEA . 8BC3 MOV EBX,EAX
004D0EEC . 8BEC MOV EBP,ESP
004D0EF1 . 8BEC MOV EBP,ESP
004D0EF6 . 55 PUSH EBP
004D0EAD . 68 00000000 PUSH DWORD PTR SS:[EBP-4],I
004D0EBC . 64:89000000 MOV DWORD PTR SS:[EBP-4],I
004D0ECE . 64:89000000 MOV DWORD PTR SS:[EBP-4],I
004D0ED0 . 64:89000000 MOV DWORD PTR SS:[EBP-4],I
004D0ED7 . 64:89000000 MOV DWORD PTR SS:[EBP-4],I
004D0EDC . 64:89000000 MOV DWORD PTR SS:[EBP-4],I
004D0EE3 . 64:89000000 MOV DWORD PTR SS:[EBP-4],I
004D0EE8 . 64:89000000 MOV DWORD PTR SS:[EBP-4],I
004D0EEA . 64:89000000 MOV DWORD PTR SS:[EBP-4],I
004D0EEC . 64:89000000 MOV DWORD PTR SS:[EBP-4],I
004D0EF1 . 64:89000000 MOV DWORD PTR SS:[EBP-4],I
004D0EF6 . 64:89000000 MOV DWORD PTR SS:[EBP-4],I

Versión	Nombre(cualquiera) Serial:
2.4 Lite	27182818

De nuevo 4 seriales

```

004BCB78 r$ 55 De softDai PUSH EBP
004BCB71 . 88EC MOV EBP,ESP
004BCB73 . 6A 00 display PUSH 0
004BCB75 . 6A 00 PUSH 0
004BCB77 . 6A 00 PUSH 0 ✓ 0457 P. M.
004BCB79 . 53 PUSH EBX
004BCB7B . 8B08 MOV EBX,EAX
004BCB7C . 33C0 XOR EAX,EAX
004BCB7E . 55 PUSH EBP
004BCB7F . 68 8CCC4B00 PUSH CaptureW.004BCC8C 0452 P. M.
004BCB84 . 64:FF30 PUSH DWORD PTR FS:[EAX]
004BCB87 . 64:8920 MOV DWORD PTR FS:[EAX],ESP
004BCB88 . 8BC3 MOV EAX,EBX
004BCB8C . BA A4CC4B00 MOV EDX,CaptureW.004BCC4 0452 P. M.
004BCB91 . E8 B275F4FF CALL CaptureW.00404148
004BCB95 . 74 2A JE SHORT CaptureW.004BCB2
004BCB98 . 8BC3 MOV EAX,EBX
004BCB99 . BA B4CC4B00 MOV EDX,CaptureW.004BCCB4 04 P. M.
004BCB9F . E8 A475F4FF CALL CaptureW.00404148 x64d...
004BCBAA . ~74 1C JE SHORT CaptureW.004BCB2
004BCBAA . 8BC3 MOV EAX,EBX
004BCBAA . BA C4CC4B00 MOV EDX,CaptureW.004BCCC4 04 P. M.
004BCBAA . E8 9675F4FF CALL CaptureW.00404148
004BCB2 . 74 0E JE SHORT CaptureW.004BCB2
004BCB4 . 8BC3 MOV EAX,EBX
004BCB6 . BA D8CC4B00 MOV EDX,CaptureW.004BCCD8 lun
004BCB8B . E8 8875F4FF CALL CaptureW.00404148
004BCB8C . ~75 08 JNZ SHORT CaptureW.004BCB24
004BCB8C > 83C4 FF OR EBX,FFFFFFFF
004BCB8C5 . ~E9 A7000000 JNP CaptureW.004BCC71
004BCB8C . > 8BC3 MOV EAX,EBX
004BCBCC . E8 6774F4FF CALL CaptureW.00404038
004BCBD1 . 83F8 08 CMP EAX,8
004BCBD4 . ~0F85 87000000 JNZ CaptureW.004BCC61
004BCBDA . 8D45 F8 LEA EAX,WORD PTR SS:[EBP-8]

```

Enter password

When you buy CaptureWiz, you get a password from tech support. Enter this password below to turn off no screens.

Tip - illegal passwords may not work with this machine, user names and passwords don't risk the security of your computer.

Your name:

Password:

module ntdll]

Thank you

Thank you for buying CaptureWizLite!

Be smart - print and save your passwords in a safe place outside this computer.

Also, please consider sending your friends a link to the free-trial - just click Help / Send a Friend a Link.

Thanks! - Dave Eisler

Versión	Nombre(cualquiera) Serial:
3.1	01650763

Aquí el mismo método, pero el call

004ACA51	<pre> . 83CA FF N OR EDX,FFFFFFF 004ACA54 . E8 8F170300 CALL CaptureW.004DE1E8 004ACA59 . 8BF0 MOV ESI,EAX 004ACA5B > 85F6 TEST ESI,ESI 004ACA5D .~ 0F8D CB000000 JGE CaptureW.004ACB2E 004ACA63 . 83FE FF CMPS ESI,-1 004ACA66 .~ 75 0F JNZ SHORT CaptureW.004ACA77 004ACA68 . 8D45 FC LEA EAX,DWORD PTR SS:[EBP-4] 004ACA6B . BA 00CC4A00 MOV EDX,CaptureW.004ACC00 004ACA70 . EB DB73F5FF CALL CaptureW.00403E50 004ACA75 . EB 2B JMP SHORT CaptureW.004ACA2A 004ACA77 > 68 30CC4A00 PUSH CaptureW.004ACC30 004ACA7C . 8055 F0 LEA EDX,DWORD PTR SS:[EBP-10] 004ACA7F . 8BC6 MOV EAX,ESI 004ACA81 . F7D8 NEG EAX 004ACA83 . E8 50CAF5FF CALL CaptureW.004094D8 004ACA88 . FF75 F0 PUSH DWORD PTR SS:[EBP-10] 004ACA8B . 68 50CC4A00 PUSH CaptureW.004ACC50 004ACA90 . 68 60CC4A00 PUSH CaptureW.004ACC60 004ACA95 . 8D45 FC LEA EAX,DWORD PTR SS:[EBP-4] 004ACA98 . BA 04000000 MOV EDX,4 004ACA9D . E8 5676F5FF CALL CaptureW.004040F8 004ACA92 > FF75 FC PUSH DWORD PTR SS:[EBP-4] 004ACA95 . 68 60CC4A00 PUSH CaptureW.004ACC60 004ACA9A . 68 78CC4A00 PUSH CaptureW.004ACC78 004ACA9F . 68 6CCC4A00 PUSH CaptureW.004ACC6C 004ACAB4 . 68 ACCC4A00 PUSH CaptureW.004ACCAC 004ACAB0 . 68 60CC4A00 PUSH CaptureW.004ACC6C </pre>	<p>Normal Título 1 Sin espacio Título 2 Título 3 Estilos</p> <p>Palabras referencias a buscar "register" que hace alusión a gracias por registrar.. arriba esta el call con el serial valido</p> <p>ASCII "Thank you for buying CaptureWizPro!"</p> <p>004ACA51 . 83CA FF N OR EDX,FFFFFFF 004ACA54 . E8 8F170300 CALL CaptureW.004DE1E8 004ACA59 . 8BF0 MOV ESI,EAX 004ACA5B > 85F6 TEST ESI,ESI 004ACA5D .~ 0F8D CB000000 JGE CaptureW.004ACB2E 004ACA63 . 83FE FF CMPS ESI,-1 004ACA66 .~ 75 0F JNZ SHORT CaptureW.004ACA77 004ACA68 . 8D45 FC LEA EAX,DWORD PTR SS:[EBP-4] 004ACA6B . BA 00CC4A00 MOV EDX,CaptureW.004ACC00 004ACA70 . EB DB73F5FF CALL CaptureW.00403E50 004ACA75 . EB 2B JMP SHORT CaptureW.004ACA2A 004ACA77 > 68 30CC4A00 PUSH CaptureW.004ACC30 004ACA7C . 8055 F0 LEA EDX,DWORD PTR SS:[EBP-10] 004ACA7F . 8BC6 MOV EAX,ESI 004ACA81 . F7D8 NEG EAX 004ACA83 . E8 50CAF5FF CALL CaptureW.004094D8 004ACA88 . FF75 F0 PUSH DWORD PTR SS:[EBP-10] 004ACA8B . 68 50CC4A00 PUSH CaptureW.004ACC50 004ACA90 . 68 60CC4A00 PUSH CaptureW.004ACC60 004ACA95 . 8D45 FC LEA EAX,DWORD PTR SS:[EBP-4] 004ACA98 . BA 04000000 MOV EDX,4 004ACA9D . E8 5676F5FF CALL CaptureW.004040F8 004ACA92 > FF75 FC PUSH DWORD PTR SS:[EBP-4] 004ACA95 . 68 60CC4A00 PUSH CaptureW.004ACC60 004ACA9A . 68 78CC4A00 PUSH CaptureW.004ACC78 004ACA9F . 68 6CCC4A00 PUSH CaptureW.004ACC6C 004ACAB4 . 68 ACCC4A00 PUSH CaptureW.004ACCAC 004ACAB0 . 68 60CC4A00 PUSH CaptureW.004ACC6C</p> <p>ASCII "Thank you for buying a "</p> <p>004ACA51 . 83CA FF N OR EDX,FFFFFFF 004ACA54 . E8 8F170300 CALL CaptureW.004DE1E8 004ACA59 . 8BF0 MOV ESI,EAX 004ACA5B > 85F6 TEST ESI,ESI 004ACA5D .~ 0F8D CB000000 JGE CaptureW.004ACB2E 004ACA63 . 83FE FF CMPS ESI,-1 004ACA66 .~ 75 0F JNZ SHORT CaptureW.004ACA77 004ACA68 . 8D45 FC LEA EAX,DWORD PTR SS:[EBP-4] 004ACA6B . BA 00CC4A00 MOV EDX,CaptureW.004ACC00 004ACA70 . EB DB73F5FF CALL CaptureW.00403E50 004ACA75 . EB 2B JMP SHORT CaptureW.004ACA2A 004ACA77 > 68 30CC4A00 PUSH CaptureW.004ACC30 004ACA7C . 8055 F0 LEA EDX,DWORD PTR SS:[EBP-10] 004ACA7F . 8BC6 MOV EAX,ESI 004ACA81 . F7D8 NEG EAX 004ACA83 . E8 50CAF5FF CALL CaptureW.004094D8 004ACA88 . FF75 F0 PUSH DWORD PTR SS:[EBP-10] 004ACA8B . 68 50CC4A00 PUSH CaptureW.004ACC50 004ACA90 . 68 60CC4A00 PUSH CaptureW.004ACC60 004ACA95 . 8D45 FC LEA EAX,DWORD PTR SS:[EBP-4] 004ACA98 . BA 04000000 MOV EDX,4 004ACA9D . E8 5676F5FF CALL CaptureW.004040F8 004ACA92 > FF75 FC PUSH DWORD PTR SS:[EBP-4] 004ACA95 . 68 60CC4A00 PUSH CaptureW.004ACC60 004ACA9A . 68 78CC4A00 PUSH CaptureW.004ACC78 004ACA9F . 68 6CCC4A00 PUSH CaptureW.004ACC6C 004ACAB4 . 68 ACCC4A00 PUSH CaptureW.004ACCAC 004ACAB0 . 68 60CC4A00 PUSH CaptureW.004ACC6C</p> <p>ASCII " machine license!"</p> <p>ASCII "...."</p> <p>ASCII "...."</p> <p>ASCII "Be smart - PRINT and save your passwords"</p> <p>ASCII "...."</p> <p>ASCII "in a safe place outside this computer. You may"</p> <p>ASCII "...."</p>
----------	--	---

Llama a otro call, claramente ya se ven mas validaciones

004DE1EE	<pre> . 51 PUSH ECX 004DE1EF . 51 PUSH ECX 004DE1F0 . 51 PUSH ECX 004DE1F1 . 51 PUSH ECX 004DE1F2 . 51 PUSH ECX 004DE1F3 . 53 PUSH EBX 004DE1F4 . 56 PUSH ESI 004DE1F5 . 8BF2 MOV ESI,EDX 004DE1F7 . 8BD8 MOV EBX,EAX 004DE1F9 . 33C0 XOR EAX,EAX 004DE1FB . 55 PUSH EBP 004DE1FC . 68 74E34D00 PUSH CaptureW.004DE374 004DE201 . 64:FF30 PUSH DWORD PTR FS:[EAX] 004DE204 . 64:8920 MOV DWORD PTR FS:[EAX],ESP 004DE207 . 8BC3 MOV EAX,EBX 004DE209 . E8 AEEFFFFF CALL CaptureW.004DE0BC 004DE20E . 8945 FC MOU DWORD PTR SS:[EBP-4],EAX </pre>	<p>Normal Título 1 Sin espacio Título 2 Título 3 Estilos</p> <p>004DE1EE . 51 PUSH ECX 004DE1EF . 51 PUSH ECX 004DE1F0 . 51 PUSH ECX 004DE1F1 . 51 PUSH ECX 004DE1F2 . 51 PUSH ECX 004DE1F3 . 53 PUSH EBX 004DE1F4 . 56 PUSH ESI 004DE1F5 . 8BF2 MOV ESI,EDX 004DE1F7 . 8BD8 MOV EBX,EAX 004DE1F9 . 33C0 XOR EAX,EAX 004DE1FB . 55 PUSH EBP 004DE1FC . 68 74E34D00 PUSH CaptureW.004DE374 004DE201 . 64:FF30 PUSH DWORD PTR FS:[EAX] 004DE204 . 64:8920 MOV DWORD PTR FS:[EAX],ESP 004DE207 . 8BC3 MOV EAX,EBX 004DE209 . E8 AEEFFFFF CALL CaptureW.004DE0BC 004DE20E . 8945 FC MOU DWORD PTR SS:[EBP-4],EAX</p>
----------	--	--

004DE0D0	. 64:FF30 N K	PUSH DWORD PTR FS:[EAX]	
004DE0D3	. 64:8920	MOU DWORD PTR FS:[EAX],ESP	
004DE0D6	. 8BC3	MOV EAX,EBX	
004DE0D8	. BA C4E14D00	MOV EDX,CaptureW.004DE1C4	
004DE0D9	. E8 6660F2FF	CALL CaptureW.004DE0448	
004DE0E2	. .75 08	JNZ SHORT CaptureW.004DE0E0C	
004DE0E4	. 83CB FF	OR EBX,FFFFFFF	
004DE0E7	. .E9 A7000000	JMP CaptureW.004DE193	
004DE0EC	. 8BC3	MOV EAX,EBX	
004DE0EE	. E8 455FF2FF	CALL CaptureW.004DE038	
004DE0F3	. 83F8 08	CMP EAX,8	
004DE0F6	. .OF85 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.004DE420	
004DE111	. 8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	
004DE114	. BA D8E14D00	MOV EDX,CaptureW.004DE108	
004DE119	. E8 2A60F2FF	CALL CaptureW.004DE148	
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.004DE420	
004DE135	. 8B45 F4	MOV EAX,DWORD PTR SS:[EBP-C]	
004DE138	. BA E4E14D00	MOV EDX,CaptureW.004DE1E4	

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.

module ntdll]

?

C CPU

Your name:

Password:

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

```
8 3 0000500  MOV EAX,50030
4:FF15 C0000000 CALL DWORD PTR FS:[C
2 0800      RETN 8
a      NOD
```

Versión	Nombre(cualquiera) Serial:
3.2	01650763

Ya el serial comienza a usarse en mas de una version

About CaptureWizPro

CaptureWizPro by Dave Eisler
version 3.20
Thank you for buying a single machine license!

```

00505630 . 64:FF30  PUSH DWORD PTR FS:[EAX]
00505633 . 64:8920  MOV DWORD PTR FS:[EAX],ESP
00505636 . 8BC3    MOV EAX,EBX
00505638 . BA 24575000 MOV EDX,CaptureW.00505724
0050563D . E8 26FCEFFF CALL CaptureW.00405268
00505642 . .75 08    JNZ SHORT CaptureW.0050564C
00505644 . .83CB FF  OR EBX,FFFFFFF
00505647 . .E9 A7000000 JMP CaptureW.005056F3
0050564C > 8BC3    MOV EAX,EBX
0050564E . E8 C9FAEFFF CALL CaptureW.0040511C
00505653 . .83F8 08  CMP EAX,8
00505656 . .0F85 87000000 JNZ CaptureW.005056E3
0050565C . .8D45 F8  LEA EAX,DWORD PTR SS:[EBP-8]
0050565F . .50      PUSH EAX
00505660 . .B9 03000000 MOV ECX,3
00505665 . .BA 01000000 MOV EDX,1
0050566A . .8BC3    MOV EAX,EBX
0050566C . .E8 0BFDEFFF CALL CaptureW.0040537C
00505671 . .8B45 F8  MOV EAX,DWORD PTR SS:[EBP-8]
00505674 . .BA 38575000 MOV EDX,CaptureW.00505738
00505679 . .E8 EAFBEFFF CALL CaptureW.00405268
0050567E . .75 63    JNZ SHORT CaptureW.005056E3
00505680 . .8D45 F4  LEA EAX,DWORD PTR SS:[EBP-C]

```

ASCII "01650763" Version 3.20

About CaptureWizPro by Dave Eisler
version 3.20
Thank you for buying a single machine license!

ASCII "732"

Versión	Nombre(cualquiera) Serial:
3.6	01650763

About CaptureWizPro

CaptureWizPro by Dave Eisler
version 3.60
Thank you for buying a single machine license!

```

00522A7C MOV EDX,CaptureW.00522B78
00522A8A MOV EDX,CaptureW.00522B8C
00522AC6 MOV EDX,CaptureW.00522BA0
00522B78 ASCII "01650763",0

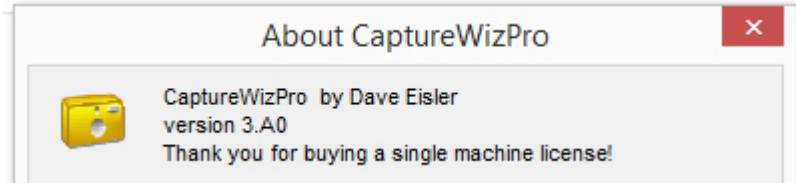
```

ASCII "01650763"

ASCII "88541853"

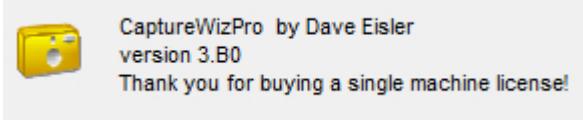
ASCII "732"

Versión	Nombre(cualquiera) Serial:
3.6A0	01650763



```
00526A6C MOV EDX,CaptureW.00526B68 ASCII "01650763"
00526A7A MOV EDX,CaptureW.00526B7C ASCII "88541853"
00526AB6 MOV EDX,CaptureW.00526B90 ASCII "732"...
```

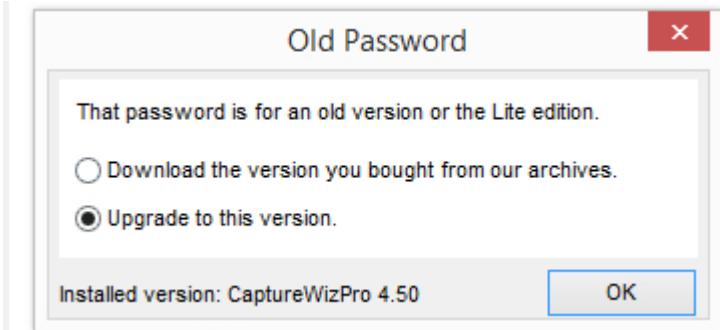
Versión	Nombre(cualquiera) Serial:
3.6A0	01650763



```
00523A88 MOV EDX,CaptureW.00523B84 ASCII "01650763"
00523A96 MOV EDX,CaptureW.00523B98 ASCII "88541853"
00523AD2 MOV EDX,CaptureW.00523BAC ASCII "732"...
```

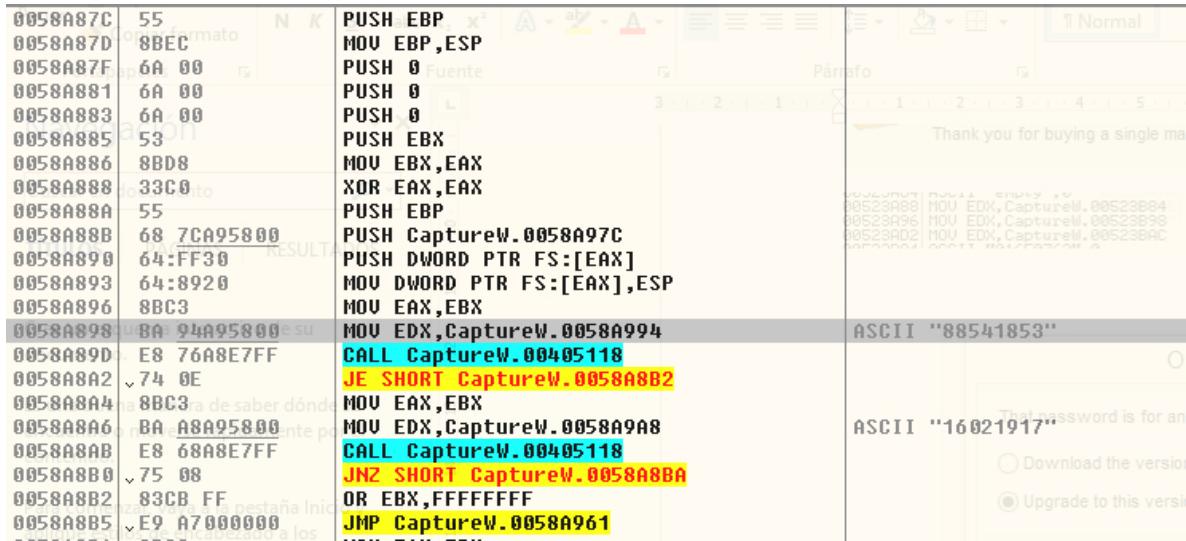
Versión	Nombre(cualquiera) Serial:
4.5	88541853

29979245, 27182818, 2718, 27182818, 01650763 muestra:



```
005333DF MOV EDX,CaptureW.00533750 ASCII "2997"
005333FC MOV EDX,CaptureW.00533760 ASCII "29979245"
00533419 MOV EDX,CaptureW.00533774 ASCII "2718"
00533436 MOV EDX,CaptureW.00533784 ASCII "27182818"
00533453 MOV EDX,CaptureW.00533798 ASCII "01650763"
0053359D IMUL EBP, DWORD PTR DS:[ESI+67], 206120 UNICODE "(Madagasikara)"
0053380D MOV EAX,CaptureW.00533828 ASCII "/BuyNow/LostPswdDscnt.php"
00533B1A MOV ECX,CaptureW.00533D44 ASCII " days left in free trial"
00533B29 PUSH CaptureW.00533D68 ASCII "Free trial expired"
00533B3E PUSH CaptureW.00533D84 ASCII " days ago"
00533B5A MOV EDX,CaptureW.00533D98 ASCII "Thank you for buying a single machine license!"
```

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



The screenshot shows a debugger interface with assembly code and a message box. The assembly code is as follows:

```
0058A87C 55          PUSH EBP
0058A87D 8BEC        MOV EBP,ESP
0058A87F 6A 00        PUSH 0
0058A881 6A 00        PUSH 0
0058A883 6A 00        PUSH 0
0058A885 53          PUSH EBX
0058A886 8BD8        MOV EBX,EAX
0058A888 33C0        XOR EAX,EAX
0058A88A 55          PUSH EBP
0058A88B 68 7CA95800 PUSH CaptureW.0058A97C
0058A890 64:FF30    PUSH DWORD PTR FS:[EAX]
0058A893 64:8920    MOV DWORD PTR FS:[EAX],ESP
0058A896 8BC3        MOV EAX,EBX
0058A898 BA 94A95800 MOV EDX,CaptureW.0058A994 ASCII "88541853"
0058A89D E8 76A8E7FF CALL CaptureW.00405118
0058A8A2 74 0E        JE SHORT CaptureW.0058A882
0058A8A4 8BC3        MOV EAX,EBX
0058A8A6 BA A8A95800 MOV EDX,CaptureW.0058A9A8 ASCII "16021917"
0058A8A8 E8 68A8E7FF CALL CaptureW.00405118
0058A8B0 75 08        JNZ SHORT CaptureW.0058A88A
0058A8B2 83CB FF    OR EBX,FFFFFF
0058A8B5 E9 A7000000 JMP CaptureW.0058A961
```

The message box content is:

Thank you for buying a single ma
00523A88 MOV EDX,CaptureW.00523A88
00523A96 MOV EDX,CaptureW.00523A96
00523A02 MOV EDX,CaptureW.00523A02
Thank you for buying CaptureWizPro
Your name: apuromaf
Password: 88541853
Administrator access required.
Passwords can't be set via Remote Desktop.
The password was successfully set.
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, author

→ The password was successfully set.

Thank you



Thank you for buying CaptureWizPro!

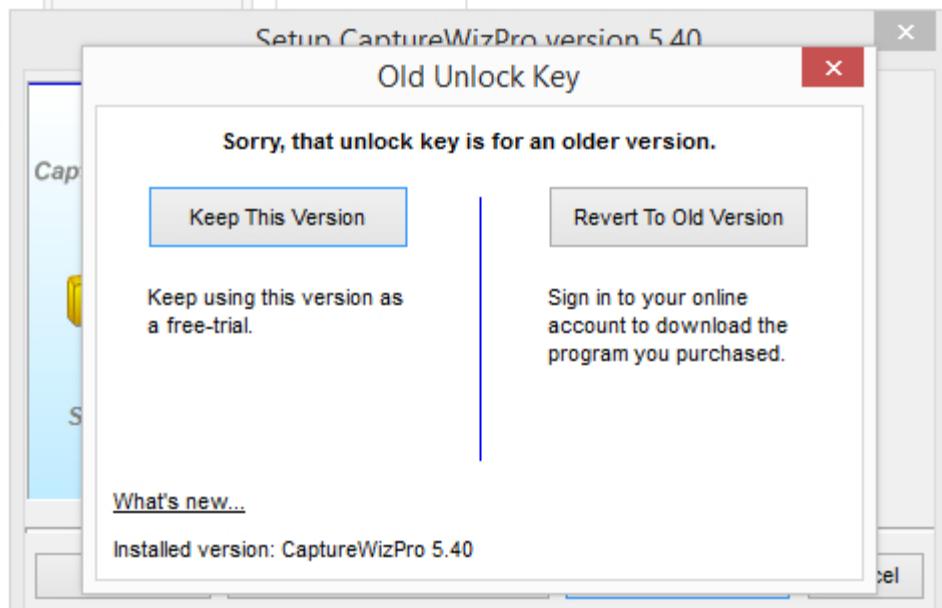
Be smart - PRINT and save your passwords in a safe place outside this computer. You may need them later to restore your computer.

Also, let your friends know about our free trial!
Click Help / Send a Friend a Link.

Thanks! - Dave, author

Versión	Nombre(cualquiera) Serial:
4.5	88541853

Con el serial anterior 88541853



```

30631301 ASCII "Sender"
30631312 ASCII "TfrmPswdOld"
30631329 ASCII "PswdOld"
30631344 UNICODE "2997",0
3063135C UNICODE "29979245"
3063136C UNICODE 0
3063137C UNICODE "2718",0
30631394 UNICODE "27182818"
306313A4 UNICODE 0
306313B4 UNICODE "01650763"
306313C4 UNICODE 0
306313D4 UNICODE "88541853"
306313E4 UNICODE 0
30631462 MOV EDX,CaptureW.00631618

```

Unlock key: 16021917

Lookup unlock key

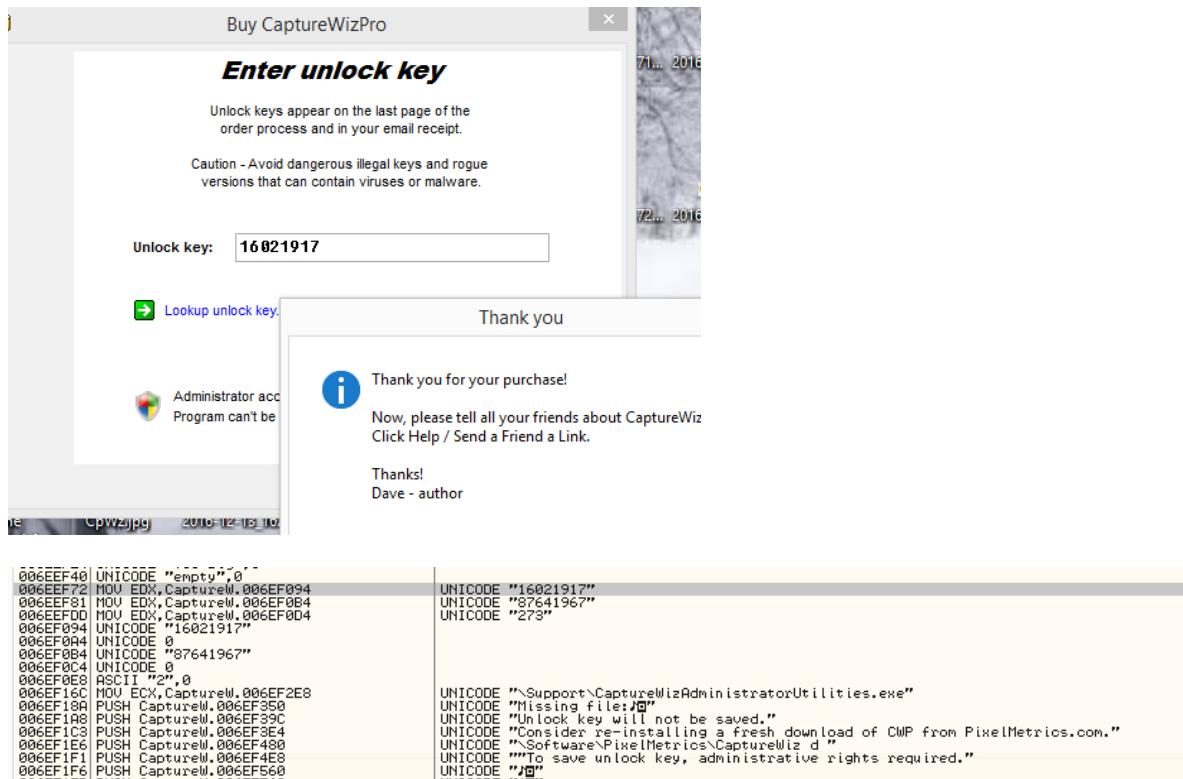
Administrator acc
Program can't be
run as an administrator.

Thank you for
purchasing this
program.

Now, please
Click Help /

UNICODE "Instal

Probamos el segundo que no verificamos: 16021917

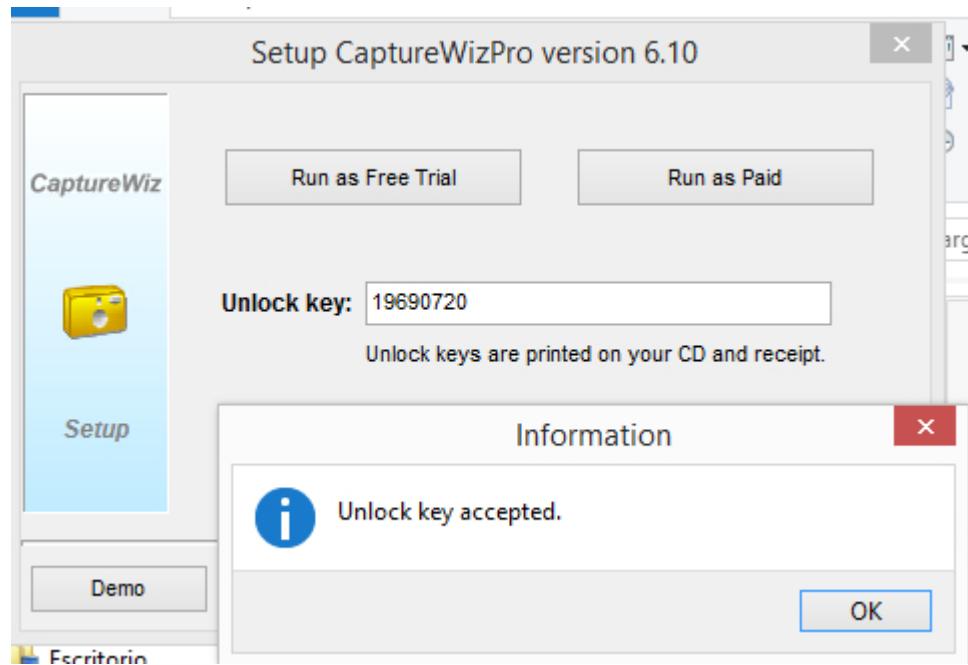


Y como hemos de suponer el segundo serial es para la próxima versión (19690720) si siguen al mismo ritmo

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 alguno 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 ☺

