



# CaptureWiz

[Escriba el subtítulo del documento]

Buscando registrarnos

13/12/2016

<b>Programa</b>	CaptureWiz (Pro) / (Lite)
<b>Protección</b>	Serial
<b>Descarga</b>	<a href="http://pixelmetrics.com/CapWizPro/Download.htm">http://pixelmetrics.com/CapWizPro/Download.htm</a> <a href="http://www.pixelmetrics.com/CapWizLite/Download.htm">http://www.pixelmetrics.com/CapWizLite/Download.htm</a>  variada:  <a href="http://pixelmetrics.com/Homepage/Downloads.htm">http://pixelmetrics.com/Homepage/Downloads.htm</a>
<b>Descripción</b>	Capturador de Pantalla
<b>Herramienta</b>	Ollydbg+ Tiempo
<b>Objetivo</b>	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 refería era el primer programa que reversaba

[https://web.archive.org/web/20120211103653/http://www.reversinglabs.com.ar/ncr/tutoriales/01-capwizpro\\_+NCR.rar](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

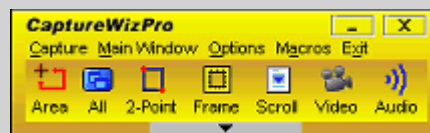
[CaptureWizPro 5.4](#)



[CaptureWizPro 4.5](#)



[CaptureWizPro 3.B](#)



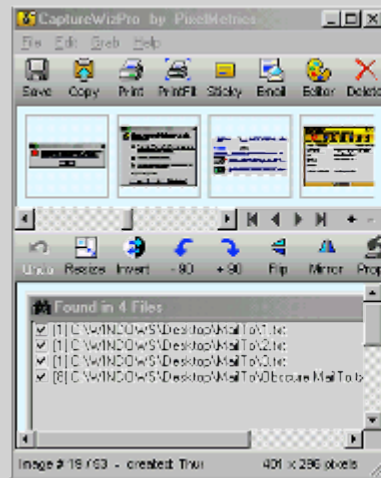
[CaptureWizPro 3.A](#)

Same appearance as 3.B above

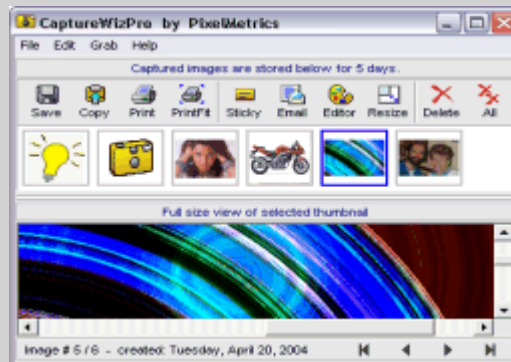
[CaptureWizPro 3.6](#)

Same appearance as 3.B above

[CaptureWizPro 3.2](#)



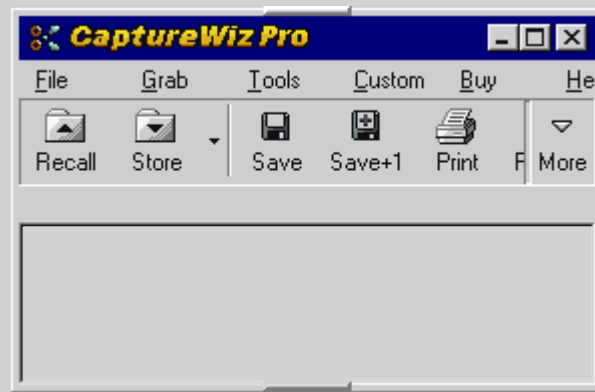
[CaptureWizPro 3.1](#)



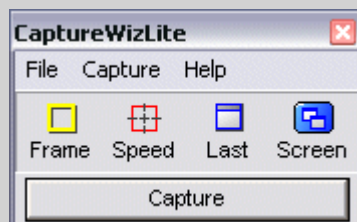
[CaptureWizPro 2.3](#)



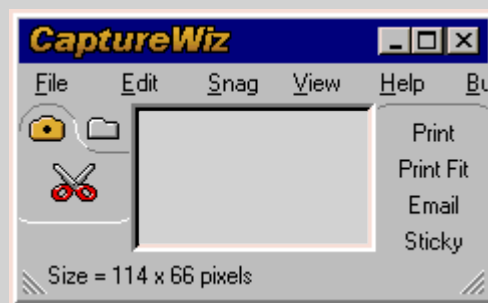
[CaptureWizPro 1.32](#)



[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):

0067392C	53	PUSH EBX
0067392D	8BD8	MOV EBX,EAX
0067392F	A1 845B7300	MOV EAX,DWORD PTR DS:[735B84]
00673934	8B00	MOV EAX,DWORD PTR DS:[EAX]
00673936	E8 00000000	CALL CaptureW.00714518
00673938	85C0	TEST EAX,EAX
0067393D	7C 0E	JL SHORT CaptureW.0067394D
0067393F	8BD3	MOV EDX,EBX
00673941	B8 02000000	MOV EAX,2
00673946	E8 5581FBFF	CALL CaptureW.00628AA0
0067394B	5B	POP EBX
0067394C	C3	RETN
0067394D	6A 00	PUSH 0
0067394F	6A FF	PUSH -1
00673951	6A FF	PUSH -1
00673953	6A 00	PUSH 0
00673955	0FB700 6C3967	MOVZX ECX,WORD PTR DS:[67396C]
0067395C	B2 02	MOV DL,2
0067395E	B8 7C396700	MOV EAX,CaptureW.0067397C
00673963	E8 14BDE5FF	CALL CaptureW.004CF67C
00673968	5B	POP EBX
00673969	C3	RETN

Arg4 = 00000000  
Arg3 = FFFFFFFF  
Arg2 = FFFFFFFF  
Arg1 = 00000000

Bueno comienzo la búsqueda  
UNICODE "Somebody already entered an unlock key, you're good to go!"  
CaptureW.004CF67C

Entonces marco la referencia del call y el salto

0067392B	00	DB 00
0067392C	53	PUSH EBX
0067392D	8BD8	MOV EBX,EAX
0067392F	A1 845B7300	MOV EAX,DWORD PTR DS:[735B84]
00673934	8B00	MOV EAX,DWORD PTR DS:[EAX]
00673936	E8 00000000	CALL CaptureW.00714518
00673938	85C0	TEST EAX,EAX
0067393D	7C 0E	JL SHORT CaptureW.0067394D
0067393F	8BD3	MOV EDX,EBX
00673941	B8 02000000	MOV EAX,2
00673946	E8 5581FBFF	CALL CaptureW.00628AA0
0067394B	5B	POP EBX
0067394C	C3	RETN
0067394D	6A 00	PUSH 0
0067394F	6A FF	PUSH -1
00673951	6A FF	PUSH -1
00673953	6A 00	PUSH 0
00673955	0FB700 6C3967	MOVZX ECX,WORD PTR DS:[67396C]
0067395C	B2 02	MOV DL,2
0067395E	B8 7C396700	MOV EAX,CaptureW.0067397C
00673963	E8 14BDE5FF	CALL CaptureW.004CF67C
00673968	5B	POP EBX
00673969	C3	RETN

1\*  
2\*

Arg4 = 00000000  
Arg3 = FFFFFFFF  
Arg2 = FFFFFFFF  
Arg1 = 00000000

Bueno comienzo la búsqueda  
UNICODE "Somebody already entered an unlock key, you're good to go!"  
CaptureW.004CF67C es que una vez ingresada la clave, no puedes volver a ingresar la clave:

Al entrar al call encuentro 2 valores

00714518	55	PUSH EBP
00714519	8BEC	MOV EBP,ESP
0071451B	33C9	XOR ECX,ECX
0071451D	51	PUSH ECX
0071451E	51	PUSH ECX
0071451F	51	PUSH ECX
00714520	51	PUSH ECX
00714521	53	PUSH EBX
00714522	8945 FC	MOV DWORD PTR SS:[EBP-4],EAX
00714525	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]
00714528	E8 9330CFFF	CALL CaptureW.004075C0
0071452D	33C0	XOR EAX,EAX
0071452F	55	PUSH EBP
00714530	68 46467100	PUSH CaptureW.00714646
00714535	64:FF30	PUSH DWORD PTR FS:[EAX]
00714538	64:8920	MOV DWORD PTR FS:[EAX],ESP
0071453B	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]
0071453E	BA 60467100	MOV EDX,CaptureW.00714660
00714543	E8 1838CFFF	CALL CaptureW.00407D60
00714548	74 0F	JE SHORT CaptureW.00714559
0071454A	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]
0071454D	BA 80467100	MOV EDX,CaptureW.00714680
00714552	E8 0938CFFF	CALL CaptureW.00407D60
00714557	75 08	JNZ SHORT CaptureW.00714561
00714559	83CB FF	OR EBX,FFFFFFFF

Bueno comienzo la búsqueda  
Lo primero que encuentro es que una vez ing  
UNICODE "87690720"  
UNICODE "19690720"

Entonces marco la referencia del call y el salto

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

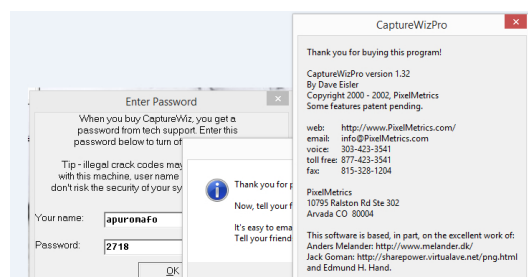
Palabras referencias a buscar “Buy” que hace alusión a gracias por registrar..un salto mas arriba esta el call con el serial valido

00498420	8BC0	MUOV EAX,EAX		OpenOffice	Image
0049842C	55	PUSH EBP		Oracle	3D
0049842D	8BEC	MUOV EBP,ESP		Oracle	CopyBitmap
0049842F	51	PUSH ECX		Oracle Technology	CopyFit
00498430	53	PUSH EBX		Passcovery	CopyFormat
00498431	8945 FC	MUOV DWORD PTR SS:[EBP-4],EAX		PasswordLastic	CopyHtml
00498434	8045 FC	MUOV EAX,DWORD PTR SS:[EBP-4]		PDLL	CwDataPath
00498437	E8 90BCF6FF	CALL CaptureW.004040CC		PE_Kill	EditorPath
0049843C	33C0	XOR EAX,EAX		Pelagian Software	Height
0049843E	55	PUSH EBP		PELock	ImagePath
0049843F	68 AD844900	PUSH CaptureW.004984AD		PHPMaker	JpgCompression
00498444	64:FF30	PUSH DWORD PTR FS:[EAX]		Pinform	LastCapFolder
00498447	64:8920	MUOV DWORD PTR FS:[EAX],ESP		PixelMetrics	ASCII "2997"
0049844A	33DB	XOR EBX,EBX		CaptureWiz	
0049844C	8B45 FC	MUOV EAX,DWORD PTR SS:[EBP-4]		Poikosoft	
0049844F	BA C4844900	MUOV EDX,CaptureW.004984C4			
00498454	E8 CFBBF6FF	CALL CaptureW.00404028			
00498459	75 3C	JNZ SHORT CaptureW.00498497			

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

588	68 00	PUSH 0		your name	ajuronafo	
589	53	PUSH EBX		Password	27182018	
58E	33C0	XOR EAX,EAX				
590	55	PUSH EBP				
591	68 17574000	PUSH CaptureW.00405717				
596	64:FF30	PUSH DWORD PTR FS:[EAX]				
599	64:8920	MUOV DWORD PTR FS:[EAX],ESP				
59C	E8 23720000	CALL CaptureW.004067C4				
5A1	8BD8	MUOV EBX,EAX				
5A3	83FB FF	CMOV EBX,-1				
5A6	75 0F	JNZ SHORT CaptureW.00405507				
5A8	8045 FC	LEA EAX,DWORD PTR SS:[EBP-4]				
5AB	BA 60574000	MUOV EDX,CaptureW.0040572C				ASCII "This program has not yet been purchased."
5B0	E8 8FE7FAFF	CALL CaptureW.00406B04				
5B5	EB 42	JMP SHORT CaptureW.004055F9				
5B7	> 85D0	TEST EBX,EBX				
5B9	75 0F	JNZ SHORT CaptureW.004055CA				
5BB	8045 FC	LEA EAX,DWORD PTR SS:[EBP-4]				
5BE	BA 60574000	MUOV EDX,CaptureW.00405760				ASCII "Thank you for buying this program!"
5C3	E8 7CE7FAFF	CALL CaptureW.00406B04				
5C8	EB 2F	JMP SHORT CaptureW.004055F9				
5CA	68 8C574000	PUSH CaptureW.0040578C				ASCII "Temporary password expires "
5CF	895D F4	MUOV DWORD PTR SS:[EBP-C],EBX				
5D2	DA45 F4	FILD DWORD PTR SS:[EBP-C]				
004BC7C4	A1 DCFD4C00	MUOV EAX,DWORD PTR DS:[4CFDDC]				
004BC7C9	8B00	MUOV EAX,DWORD PTR DS:[EAX]				
004BC7CB	BA F0C74000	MUOV EDX,CaptureW.004BC7F0				ASCII "2718"
004BC7D0	E8 6778F4FF	CALL CaptureW.0040403C				
004BC7D5	75 03	JNZ SHORT CaptureW.004BC7D8				
004BC7D7	33C0	XOR EAX,EAX				
004BC7D9	C3	RET				
004BC7DA	A1 DCFD4C00	MUOV EAX,DWORD PTR DS:[4CFDDC]				
004BC7DF	8B00	MUOV EAX,DWORD PTR DS:[EAX]				
004BC7E1	E8 9AFEFFFF	CALL CaptureW.004BC680				
004BC7E6	C3	RET				
004BC7E7	00	DB 00				
004BC7E8	FFFFFF	DD FFFFFFFF				





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	ASCII "2718"
004D0EC9	E8 7A32F3FF	CALL CaptureW.00404148	Versión
004D0ECE	74 2A	JE SHORT CaptureW.004D0EFA	No
004D0ED0	8BC3	MOV EAX,EBX	Ser
004D0ED2	BA EC0F4D00	MOV EDX,CaptureW.004D0FEC	295
004D0ED7	E8 6C32F3FF	CALL CaptureW.00404148	
004D0EDC	8BC3	MOV EAX,EBX	
004D0EDE	BA FC0F4D00	MOV EDX,CaptureW.004D0FFC	
004D0EE3	E8 6032F3FF	CALL CaptureW.00404148	
004D0EE8	74 10	JE SHORT CaptureW.004D0EFA	
004D0EEA	8BC3	MOV EAX,EBX	
004D0EEC	BA 10104D00	MOV EDX,CaptureW.004D1010	
004D0EF1	E8 5232F3FF	CALL CaptureW.00404148	
004D0EF6	75 0A	JNZ SHORT CaptureW.004D0F02	

Versión	Nombre(cualquiera) Serial:
2.4 Lite	27182818

De nuevo 4 seriales

0040CB70	55	PUSH EBP	
0040CB71	8BEC	MOV EBP,ESP	
0040CB73	6A 00	PUSH 0	
0040CB75	6A 00	PUSH 0	
0040CB77	6A 00	PUSH 0	
0040CB79	53	PUSH EBX	
0040CB7A	8BD8	MOV EBX,EAX	
0040CB7C	33C0	XOR EAX,EAX	
0040CB7E	55	PUSH EBP	
0040CB7F	68 8CCC4B00	PUSH CaptureW.0040BCC8C	
0040CB84	64:FF30	PUSH DWORD PTR FS:[EAX]	
0040CB87	64:8920	MOV DWORD PTR FS:[EAX],ESP	
0040CB8A	8BC3	MOV EAX,EBX	
0040CB8C	BA A4CC4B00	MOV EDI,CaptureW.0040BCCA4	ASCII "2718"
0040CB91	E8 B275F4FF	CALL CaptureW.00404148	
0040CB96	74 2A	JE SHORT CaptureW.0040B8C2	
0040CB98	8BC3	MOV EAX,EBX	
0040CB9A	BA B4CC4B00	MOV EDI,CaptureW.0040BCCB4	ASCII "2997"
0040CB9F	E8 A475F4FF	CALL CaptureW.00404148	
0040CBA4	74 1C	JE SHORT CaptureW.0040B8C2	
0040CBA6	8BC3	MOV EAX,EBX	
0040CBA8	BA C4CC4B00	MOV EDI,CaptureW.0040BCCC4	ASCII "27182818"
0040CBA0	E8 9675F4FF	CALL CaptureW.00404148	
0040CBB2	74 0E	JE SHORT CaptureW.0040B8C2	
0040CBB4	8BC3	MOV EAX,EBX	
0040CBB6	BA D8CC4B00	MOV EDI,CaptureW.0040BCCD8	ASCII "29979245"
0040CBB8	E8 8875F4FF	CALL CaptureW.00404148	
0040CBC0	75 08	JNZ SHORT CaptureW.0040B8CA	
0040CBC2	> 83CB FF	OR EBX,FFFFFFFF	
0040CBC5	E9 A7000000	JMP CaptureW.0040BCC71	
0040CBCA	> 8BC3	MOV EAX,EBX	
0040CBCC	E8 6774F4FF	CALL CaptureW.00404038	
0040CBD1	83F8 08	CMP EAX,8	
0040CBD4	0F85 87000000	JNZ CaptureW.0040BCC61	
0040CDDA	8D45 F8	LEA EAX,DWORD PTR SS:[EBP-8]	

## 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 cause problems with this machine, user name and password don't risk the security of your system.

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

Acepta

Versión	Nombre(cualquiera) Serial:
3.1	01650763

Aquí el mismo método, pero el call

004ACA51	. 83CA FF	OR EDX,FFFFFFFF	
004ACA54	. E8 8F170300	CALL CaptureW.004DE1E8	
004ACA59	. 8BF0	MOV ESI,EAX	
004ACA5B	> 85F6	TEST ESI,ESI	
004ACA5D	. 0F8D C8000000	JGE CaptureW.004ACB2E	
004ACA63	. 83FE FF	CMP 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	. E8 DB73F5FF	CALL CaptureW.00403E50	
004ACA75	. EB 2B	JMP SHORT CaptureW.004ACAA2	
004ACA77	> 68 30CC4A00	PUSH CaptureW.004ACC30	
004ACA7C	. 8D55 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 6CCC4A00	PUSH CaptureW.004ACC6C	
004ACA95	. 8D45 FC	LEA EAX,DWORD PTR SS:[EBP-4]	
004ACA98	. BA 0A000000	MOV EDX,4	
004ACA9D	. E8 5676F5FF	CALL CaptureW.004040F8	
004ACAA2	> FF75 FC	PUSH DWORD PTR SS:[EBP-4]	
004ACAA5	. 68 6CCC4A00	PUSH CaptureW.004ACC6C	
004ACAA8	. 68 78CC4A00	PUSH CaptureW.004ACC78	
004ACAAF	. 68 6CCC4A00	PUSH CaptureW.004ACC6C	
004ACAB4	. 68 ACCC4A00	PUSH CaptureW.004ACCAC	
004ACAB9	. 68 6CCC4A00	PUSH CaptureW.004ACC6C	

Palabras referencias a buscar "register" que hace alusión a gracias por registrar.

Arriba esta el call con el serial valido

ASCII "Thank you for buying CaptureWizPro!"

ASCII "Thank you for buying a "

ASCII " machine license!"

ASCII ""

Versión	Nombre(cualquiera)
3.1	Serial:
	2718

ASCII ""

ASCII "Be smart - PRINT and save your passwords"

ASCII ""

ASCII "in a safe place outside this computer. You may"

ASCII ""

Llama a otro call, claramente ya se ven mas validaciones

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 AEF0FFFF	CALL CaptureW.004DE0BC	*
004DE20E	. 8945 FC	MOV DWORD PTR SS:[EBP-4],EAX	

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	ASCII "01650763"
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	CMR 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	ASCII "732"
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	

## 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:

Password:

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.

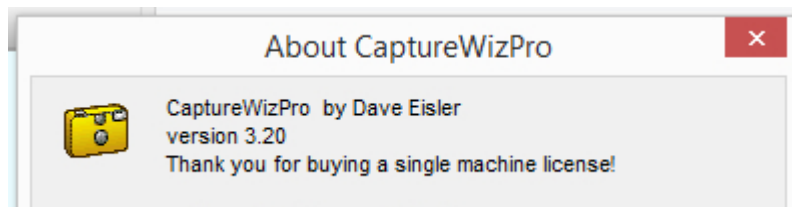
Also, let your friends know about our free-trial! Click Help / Send a Friend a Link.

Thanks! - Dave Eisler

Aceptar

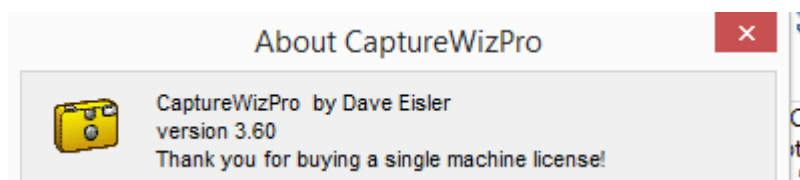
Versión	Nombre(cualquiera) Serial:
3.2	01650763

Ya el serial comienza a usarse en mas de una version



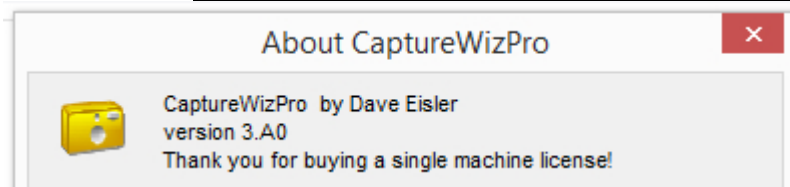
00505630	. 64:FF30	PUSH DWORD PTR FS:[EAX]	
00505633	. 64:8920	MOV DWORD PTR FS:[EAX],ESP	
00505636	. 8BC3	MOV EAX,EBX	
00505638	. BA 24575000	MOV EDX,CaptureW.00505724	
0050563D	. E8 26FCEFFF	CALL CaptureW.00405268	ASCII "01650763"
00505642	. 75 08	JNZ SHORT CaptureW.0050564C	
00505644	. 83CB FF	OR EBX,FFFFFFFF	
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	ASCII "732"
00505679	. E8 EAFBEFFF	CALL CaptureW.00405268	
0050567E	. 75 63	JNZ SHORT CaptureW.005056E3	
00505680	. 8D45 F4	LEA EAX,DWORD PTR SS:[EBP-C]	

Versión	Nombre(cualquiera) Serial:
3.6	01650763



00522A7C	MOV EDX,CaptureW.00522B78	ASCII "01650763"
00522A8A	MOV EDX,CaptureW.00522B8C	ASCII "88541853"
00522AC6	MOV EDX,CaptureW.00522BA0	ASCII "732"
00522B78	ASCII "01650763",0	

Versión	Nombre(cualquiera) Serial:
3.6A0	01650763

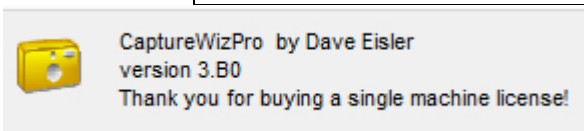


```

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



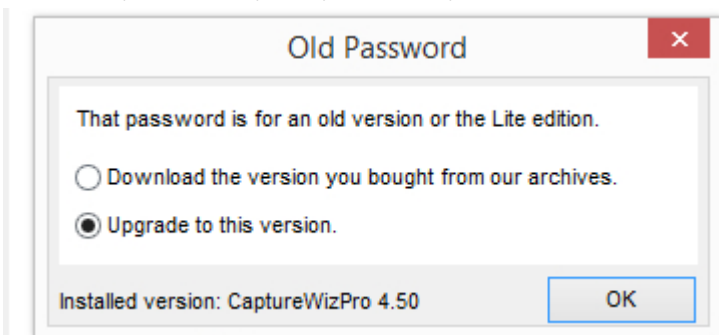
```

00523A87 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/LostPswdDsont.php"
0053381A MOV ECK,CaptureW.00533D44 ASCII " days left in free trial"
00533829 PUSH CaptureW.00533D68 ASCII "Free trial expired "
0053383E PUSH CaptureW.00533D84 ASCII " days ago"
0053385A MOV EDX,CaptureW.00533D98 ASCII "Thank you for buying a single machine license!"
0053386D MOV EDX,CaptureW.00533D9A 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

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
0058A89D	E8 76A8E7FF	CALL CaptureW.00405118
0058A8A2	74 0E	JE SHORT CaptureW.0058A8B2
0058A8A4	8BC3	MOV EAX,EBX
0058A8A6	BA A8A95800	MOV EDX,CaptureW.0058A9A8
0058A8AB	E8 68A8E7FF	CALL CaptureW.00405118
0058A8B0	75 08	JNZ SHORT CaptureW.0058A8BA
0058A8B2	83CB FF	OR EBX,FFFFFFFF
0058A8B5	E9 A7000000	JMP CaptureW.0058A961

Your name:

Password:

 Administrator access required.  
Passwords can't be set via Remote Desktop.

 The password was

Thank you



Thank you for buying CaptureWizPro!

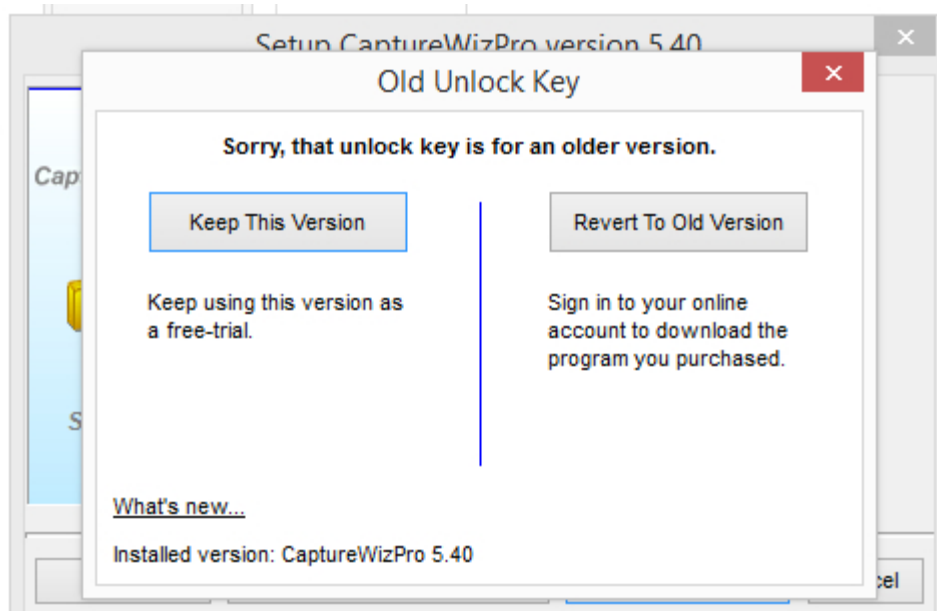
Be smart - PRINT and save your passwords  
in a safe place outside this computer. You may  
need them later to restore your computer.

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

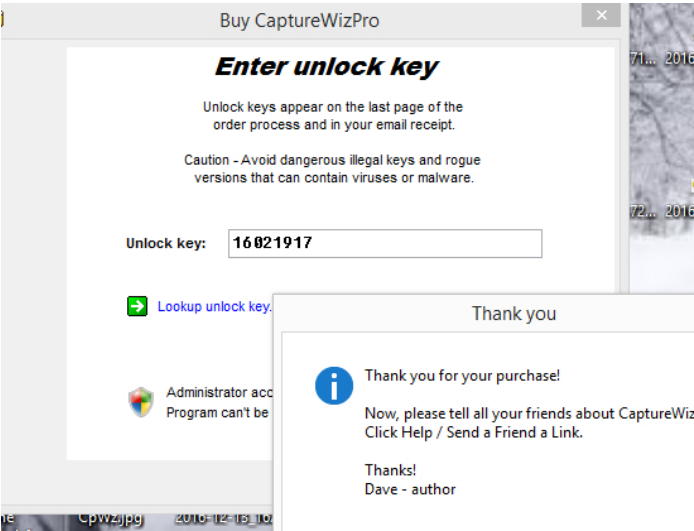
Con el serial anterior 88541853



30631301	ASCII	"Sender"	
30631312	ASCII	"TfrmPswdOld"	
30631328	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	UNICODE "Instal



Probamos el segundo que no verificamos: 16021917



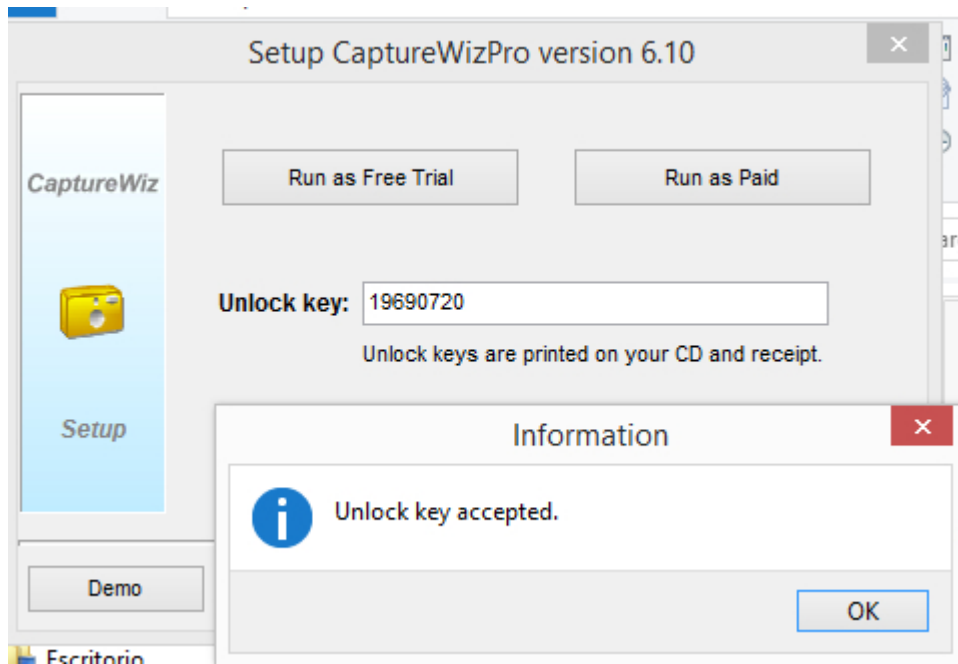
006EEF40	UNICODE "empty", 0	UNICODE "16021917"
006EEF72	MOV EDX, CaptureWiz.006EF094	UNICODE "87641967"
006EEF81	MOV EDX, CaptureWiz.006EF0B4	UNICODE "273"
006EEFDD	MOV EDX, CaptureWiz.006EF0D4	
006EF094	UNICODE "16021917"	
006EF0A4	UNICODE 0	
006EF0B4	UNICODE "87641967"	
006EF0C4	UNICODE 0	
006EF0E8	ASCII "2", 0	
006EF16C	MOV ECX, CaptureWiz.006EF2E8	UNICODE "\\Support\\CaptureWizAdministratorUtilities.exe"
006EF18A	PUSH CaptureWiz.006EF350	UNICODE "Missing file: %s"
006EF1A8	PUSH CaptureWiz.006EF39C	UNICODE "Unlock key will not be saved."
006EF1C3	PUSH CaptureWiz.006EF3E4	UNICODE "Consider re-installing a fresh download of CMP from PixelMetrics.com."
006EF1E6	PUSH CaptureWiz.006EF480	UNICODE "Software\\PixelMetrics\\CaptureWiz d"
006EF1F1	PUSH CaptureWiz.006EF4E8	UNICODE "To save unlock key, administrative rights required."
006EF1F6	PUSH CaptureWiz.006EF560	UNICODE "%s"

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 captador 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 ☺

