

Enviado a 19:28 del viernes ~peticion  
Enviado a 20:11 del viernes ~cracked

Saludos cordiales,

Primero el precio

When the trial period expires, you can register the product with an registration code sent instantly upon purchase via email. You'll get

- **Full use of HtmlCapture with no watermarks.**
- **Ordering HtmlCapture online is safe, secure and guaranteed** via [plimus!](#)
- **FREE** update for future versions
- **FREE** customer support

<input type="radio"/> IE Edition (no Firefox rendering engine)	<b>\$149.95</b>
<input checked="" type="radio"/> Standard License	<del>\$249.95</del> <b>\$199.95</b>
<input type="radio"/> Enterprise License	<b>\$899.95</b>

**Buy Now!**

[Download HtmlCapture v2.0 NOW](#) to Try it for FREE!

No functionality limitation except watermarks in the generated image for the unregistered version.

Y desccargo gratis xD  
version.

**Free Download!**

[Download Now](#)

**Buy Now**

When the trial period expires, you can register the product with an reg instantly upon purchase via email. You'll get

- **Full use of HtmlCapture with no watermarks.**

Encontrar:  [Siguiente](#) [Anterior](#) [Resaltar todo](#) ☐ [Coincide](#)

<http://www.polestarsoft.com/download/HtmlCaptureSetup.exe>

Si valia mas de \$20 ya es caro  
Comenzamos abriendolo en el olly

The screenshot shows the OllyDbg interface with the assembly window displaying the following code:

```
00421000 $ E8 2F510000 CALL MainDemo.00426001
00421002 ^ E9 17FEFFFF JMP MainDemo.0042101E
00421007 $ 51 PUSH ECX
00421008 ^ C701 F40D4300 MOV DWORD PTR DS:[ECX],MainDemo.0043D0F
0042100E ^ E9 82510000 CALL MainDemo.00426005
00421013 ^ 59 POP ECX
00421014 ^ C3 RETN
00421015 ^ 56 PUSH ESI
00421016 ^ 8BF1 MOV ESI,ECX
00421018 ^ E9 EAF0FFFF CALL MainDemo.00421007
0042101D ^ F64424 08 01 TEST BYTE PTR SS:[ESP+8],1
00421022 ^ 74 07 JE SHORT MainDemo.0042102B
00421024 ^ 56 PUSH ESI
00421025 ^ E9 3638FEFF CALL MainDemo.00405460
0042102A ^ 59 POP ECX
0042102B ^ 8BC6 MOV EAX,ESI
0042102D ^ C3 RETN
```

The registers window on the right shows the following values:

Register	Value	Comment
CR0	00000000	
CR2	0012FFFF	
CR3	7C91EB94	ntdll.KiF
CR4	7FFD4000	
CR8	0012FFFF	
EAX	0012FFFF	
ECX	0012FFFF	
EDX	0012FFFF	
ESI	0012FFFF	
EDI	7C920738	ntdll.7C
EIP	004210FD	MainDemo.
EAX	00000000	
ECX	0012FFFF	
EDX	7C91EB94	ntdll.KiF
EBX	7FFD4000	
ESP	0012FFFF	
EBP	0012FFFF	
ESI	0012FFFF	
EDI	7C920738	ntdll.7C
EIP	004210FD	MainDemo.
C 0	ES 0023 32bit 00f	
P 1	CS 001B 32bit 00f	
D 0	DS 0023 32bit 00f	
I 1	SS 0023 32bit 00f	
Z 1	DS 0023 32bit 00f	
S 0	FS 003B 32bit 7FF	

Tipico ap lib?  
Alt+e y ejecuto

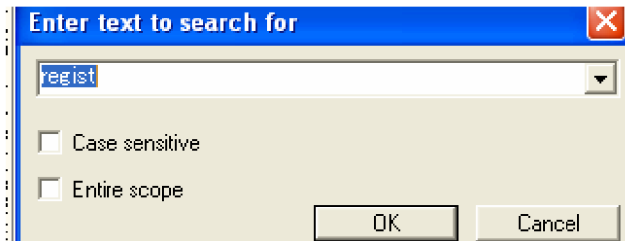
Base	Size	Entry	Name	File version	Path
00400000	0006B000	00421BFD	MainDemo	1.0.0.1	C:\Archivos de programa\XP2\HtmlCapture v2.0\MainDemo.exe
62E38000	00009000	62E32EAD	LPK	5.1.2600.2180	C:\XPSP2\system32\LPK.DLL
72F80000	00026000	72F84D00	WINSPOOL	5.1.2600.2180	C:\XPSP2\system32\WINSPOOL.DRV
74CC0000	00020000	74CC13FA	oledlg	1.0 (XPC)lient.0	C:\XPSP2\system32\oledlg.dll
74D20000	0006B000	74D5AEB6	USP10	1.0420.2600.2180	C:\XPSP2\system32\USP10.dll
76340000	00010000	763412C8	IMM32	5.1.2600.2180	C:\XPSP2\system32\IMM32.DLL
76360000	0004A000	76361AB8	condlg32	6.00.2900.2180	C:\XPSP2\system32\condlg32.dll
770F0000	0000C000	770F1558	OLEAUT32	5.1.2600.2180	C:\XPSP2\system32\OLEAUT32.dll
77300000	00102000	773042B9	COMCTL32	6.0 (Xpsp_sp2_r	C:\XPSP2\WinSxS\Win6_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2.0_x-ww_6595b64144ccf1df_x-ww_6595b64144ccf1df\COMCTL32.dll
77480000	0018C000	774C20C1	ole32	5.1.2600.2180	C:\XPSP2\system32\ole32.dll
77BE0000	00058000	77BEF2A1	msvcrt	7.0.2600.2180	C:\XPSP2\system32\msvcrt.dll
77D10000	00090000	77D20EB9	USER32	5.1.2600.2180	C:\XPSP2\system32\USER32.dll
77DA0000	000AC000	77DA70D4	ADVAPI32	5.1.2600.2180	C:\XPSP2\system32\ADVAPI32.dll
77E50000	00091000	77E56284	RPCRT4	5.1.2600.2180	C:\XPSP2\system32\RPCRT4.dll
77F90000	00046000	77F963CA	GDI32	5.1.2600.2180	C:\XPSP2\system32\GDI32.dll
77FA0000	00076000	77FA51D3	SHLWAPI	6.00.2900.2180	C:\XPSP2\system32\SHLWAPI.dll
7C800000	00101000	7C80B436	kernel32	5.1.2600.2180	C:\XPSP2\system32\kernel32.dll
7C910000	00066000	7C923156	ntdll	5.1.2600.2180	C:\XPSP2\system32\ntdll.dll
7C9D0000	00081E000	7C9EFA10	SHELL32	6.00.2900.2180	C:\XPSP2\system32\SHELL32.dll

Ejecutado

Base	Size	Entry	Name	File version	Path
00400000	0006B000	00421BFD	MainDemo	1.0.0.1	C:\Archivos de programa\XP2\HtmlCapture v2.0\MainDemo.exe
10000000	00126000	1009CD19	HtmlCapt	2.0.62.0	C:\Archivos de programa\XP2\HtmlCapture v2.0\HtmlCapture.dll
5B150000	00038000	5B151626	uxtheme	6.00.2900.2180	C:\XPSP2\system32\uxtheme.dll
62E38000	00009000	62E32EAD	LPK	5.1.2600.2180	C:\XPSP2\system32\LPK.DLL
72F80000	00026000	72F84D00	WINSPOOL	5.1.2600.2180	C:\XPSP2\system32\WINSPOOL.DRV
74CC0000	00020000	74CC13FA	oledlg	1.0 (XPC)lient.0	C:\XPSP2\system32\oledlg.dll
74D20000	0006B000	74D5AEB6	USP10	1.0420.2600.2180	C:\XPSP2\system32\USP10.dll

Entro en la dll

Address	Hex dump	ASCII
00449000	F4 DD 43 00 00 00 00 00	11C.....
00449008	2E 3F 41 56 43 40 61 69	?AVCmai
00449010	6E 44 5D 6F 41 70 70 70	nDemoApp
00449018	40 40 00 00 00 40 43 00	@...11C
00449020	00 00 00 00 2E 3F 41 56	....?AV
00449028	43 57 69 6E 41 70 70 40	CWinApp@
00449030	40 00 00 00 F4 DD 43 00	@...11C
00449038	00 00 00 00 2E 3F 41 56	....?AV
00449040	43 57 69 6E 54 68 72 65	CWinThre
00449048	E1 64 40 40 00 00 00 00	ad@....
00449050	F4 DD 43 00 00 00 00 00	11C.....
00449058	2E 3F 41 56 43 40 61 69	?AVCnd
00449060	54 61 72 67 65 74 40 40	Target@



```

10028F44 PUSH HtmlCapt.100C1D94 UNICODE "UNICODE_Rdw"
10028F45 PUSH HtmlCapt.100C1D94 UNICODE "REGISTRY"
10028F4B MOV DWORD PTR SS:[ESP+1C],HtmlCapt.100C UNICODE "APPID"
10028FD3 MOV DWORD PTR SS:[ESP+20],HtmlCapt.100C UNICODE "C2D8F614F-EE2"
10029081 MOV DWORD PTR SS:[ESP+1C],HtmlCapt.100C UNICODE "APPID"
10029082 MOV DWORD PTR SS:[ESP+20],HtmlCapt.100C UNICODE "C2D8F614F-EE2"

```

Ctrl+ly continuo

```

10030FB7 PUSH HtmlCapt.100C1748 ASCII "():"
10030FBF PUSH HtmlCapt.100C3320 ASCII "CSnapShooter::FinalConstruct"
10030FC3 PUSH HtmlCapt.100C3308 UNICODE "unregisterd"
10030FDD PUSH HtmlCapt.100C3308 UNICODE "unregisterd"
10030F77 PUSH HtmlCapt.100C1748 ASCII "():"
10030F7F PUSH HtmlCapt.100C3340 ASCII "CSnapShooter::FinalRelease"
10030F83 PUSH HtmlCapt.100C1748 ASCII "():"
10030F8B PUSH HtmlCapt.100C335C ASCII "CSnapShooter::Error"
10030F96 PUSH HtmlCapt.100C1748 ASCII "():"
10030F97 PUSH HtmlCapt.100C3320 ASCII "CSnapShooter::Construct"

```

```

10046AAA PUSH HtmlCapt.100C4748 ASCII "12"
10046D4A PUSH HtmlCapt.100C4734 UNICODE "Arial"
10046DDA PUSH HtmlCapt.100C46E0 UNICODE "Generated by HtmlCapture ActiveX Control"
10046E2F PUSH HtmlCapt.100C46E0 UNICODE "Unregistered Version."
10046E5D PUSH HtmlCapt.100C4684 UNICODE "WWW.POLESTARSOFT.COM"
100472C3 PUSH HtmlCapt.100C1748 ASCII "():"
100472CB PUSH HtmlCapt.100C46A4 ASCII "CSnapTask::Initialize"
100483FA PUSH HtmlCapt.100C47E4 ASCII "19"
10048414 PUSH HtmlCapt.100C47E0 ASCII "37"
10049016 PUSH HtmlCapt.100C4788 UNICODE "9A4963DEE2840EE7B73391A7374157B9"
10049077 PUSH HtmlCapt.100C477C UNICODE "10001"
10049E16 PUSH HtmlCapt.100C4754 ASCII "0123456789ABCDEFGHIJKLMNPQRSTUVWXYZ?"
10049EB4 PUSH HtmlCapt.100C4750 ASCII "17"
1004A406 PUSH HtmlCapt.100C4748 ASCII "12"
1004B704 PUSH HtmlCapt.100C47E4 ASCII "19"

```

Aca comenzando la tarde llega un mj de ayuda

Supuestamente eso seria lo importante o no?

Voy alla

```

0046D06 > 33C0 XOR EAX,EAX
0046D08 > 6A 28 PUSH 28
0046D0A > 68 E0460C10 PUSH HtmlCapt.100C46E0
0046D0F > 8D4D 54 LEA ECX,DWORD PTR SS:[EBP+54]
0046DE2 > C745 6C 07000 MOV DWORD PTR SS:[EBP+6C],7
0046DE9 > 8945 68 MOV DWORD PTR SS:[EBP+68],EAX
0046DEC > 66:8945 58 MOV WORD PTR SS:[EBP+58],AX
0046DF0 > E8 2B03FCFF CALL HtmlCapt.10007120
0046DF5 > 837D 6C 08 CMP DWORD PTR SS:[EBP+6C],8
0046DF9 > 8B45 58 MOV EAX,DWORD PTR SS:[EBP+58]
0046DFC > C745 FC 27000 MOV DWORD PTR SS:[EBP+4],27
0046E03 > 73 03 JNB SHORT HtmlCapt.10046E06
0046E05 > 8D45 58 LEA EAX,DWORD PTR SS:[EBP+58]
0046E08 > 8D4D 68 MOV ECX,DWORD PTR SS:[EBP+68]
0046E0B > 8B95 84020000 MOV EDX,DWORD PTR SS:[EBP+284]
0046E11 > 8B85 80020000 MOV ESI,DWORD PTR SS:[EBP+280]

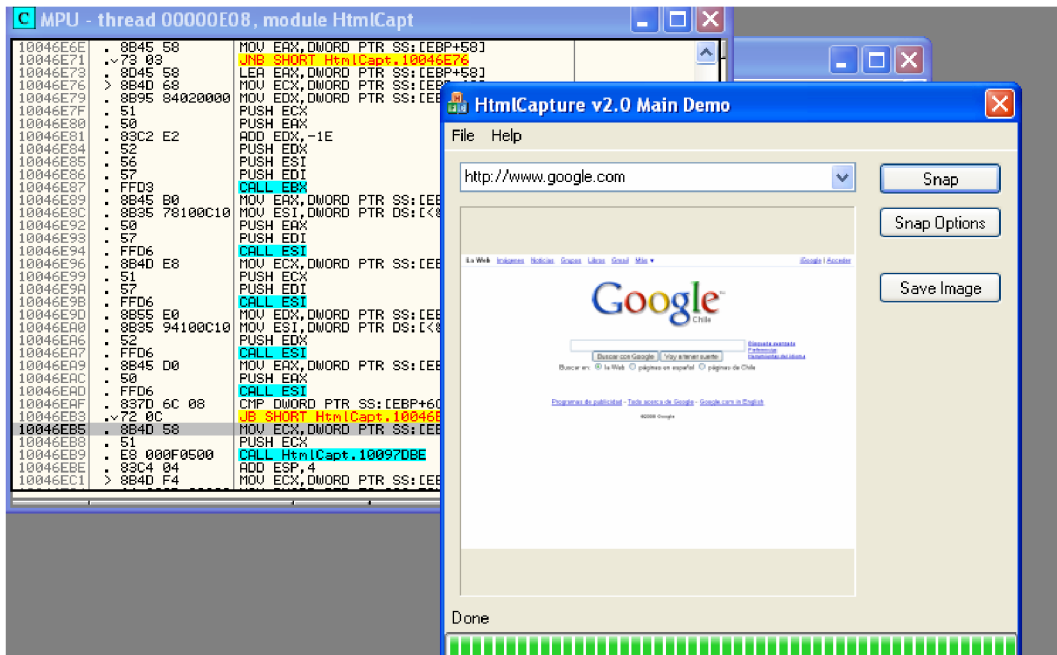
```

Donde estoy en el jnz si se cambia a jmp

10046D27	. 8B5E 20	MOV EDX,DWORD PTR SS:[EBP+20]		
10046D29	. 52	PUSH EDX		
10046D2B	. E8 8E100500	CALL Htm1Capt.100970BE		
10046D30	. 83C4 04	ADD ESP,4		
10046D33	> 8BFE	CMPL EDI,ESI		
10046D35	. 0F85 86010000	JNZ Htm1Capt.10046EC1		
10046D3B	. 68 287DF000	PUSH 0F07D28		Color = RGB(40.,125.,240.)
10046D40	. 6A 03	PUSH 3		Width = 3
10046D42	. 6A 00	PUSH 0		PenStyle = PS_SOLID
10046D44	. FF15 4C100C10	CALL DWORD PTR DS:[<&GDI32.CreatePen>]		CreatePen
10046D4A	. 68 34470C10	PUSH Htm1Capt.100C4734		FaceName = "Arial"
10046D4F	. 6A 00	PUSH 0		PitchAndFamily = DEFAULT_PITCH FF_DONTCARE
10046D51	. 6A 04	PUSH 4		Quality = 4.
10046D53	. 6A 00	PUSH 0		ClipPrecision = CLIP_DEFAULT_PRECIS
10046D55	. 6A 00	PUSH 0		OutputPrecision = OUT_DEFAULT_PRECIS
10046D57	. 6A 00	PUSH 0		CharSet = ANSI_CHARSET
10046D59	. 6A 00	PUSH 0		StrikeOut = FALSE
10046D5B	. 6A 00	PUSH 0		Underline = FALSE
10046D5D	. 6A 00	PUSH 0		Italic = FALSE
10046D5F	. 68 BC020000	PUSH 2BC		Weight = FW_BOLD
10046D64	. 6A 00	PUSH 0		Orientation = 0
10046D66	. 6A 00	PUSH 0		Escapement = 0
10046D68	. 6A 00	PUSH 0		Width = 0
10046D6A	. 8BF0	MOV ESI,EBX		Height = 10 (16.)
10046D6C	. 6A 10	PUSH 10		
10046D6E	. 8975 E0	MOV DWORD PTR SS:[EBP-20],ESI		
10046D71	. FF15 50100C10	CALL DWORD PTR DS:[<&GDI32.CreateFontW>]		CreateFontW
10046D77	. 8B7D 00	MOV EDI,DWORD PTR SS:[EBP-50]		
10046D7A	. 56	PUSH ESI		
10046D7B	. 8B35 78100C10	MOV ESI,DWORD PTR DS:[<&GDI32.SelectObject>]		hObject
10046D81	. 8BD8	MOV EBX,EBX		GDI32.SelectObject
10046D83	. 57	PUSH EDI		hDC
10046D84	. 895D 00	MOV DWORD PTR SS:[EBP-30],EBX		SelectObject
10046D87	. FFD6	CALL ESI		hObject
10046D89	. 53	PUSH EBX		hDC
10046D8A	. 57	PUSH EDI		
10046D8B	. 8945 00	MOV DWORD PTR SS:[EBP-50],EBX		SelectObject
10046D8E	. FFD6	CALL ESI		Color = <LIGHTRED>
10046D90	. 68 FF000000	PUSH 0FF		hDC
10046D95	. 57	PUSH EDI		
10046D96	. 8945 E8	MOV DWORD PTR SS:[EBP-10],EBX		
10046D99	. FF15 54100C10	CALL DWORD PTR DS:[<&GDI32.SetTextColor>]		SetTextColor
10046D9F	. 8B9D 8A020000	MOV EBX,DWORD PTR SS:[EBP+284]		
10046D83	> 8BFE	CMPL EDI,ESI		
10046D85	. E9 87010000	JMP Htm1Capt.10046EC1		
10046D8A	. 90	NOP		
10046D8B	. 68 287DF000	PUSH 0F07D28	Backup	r = RGB(40.,125.,240.)
10046D90	. 6A 03	PUSH 3	Copy	n = 3
10046D92	. 6A 00	PUSH 0	Binary	yle = PS_SOLID
10046D94	. FF15 4C100C10	CALL DWORD PTR DS:[<&GDI32.CreatePen>]		Pen
10046D9A	. 68 34470C10	PUSH Htm1Capt.100C4734		FaceName = "Arial"
10046D9F	. 6A 00	PUSH 0	Assemble	AndFamily = DEFAULT_PITCH FF_DONTCARE
10046DA1	. 6A 04	PUSH 4	Space	ity = 4.
10046DA3	. 6A 00	PUSH 0		Precision = CLIP_DEFAULT_PRECIS
10046DA5	. 6A 00	PUSH 0	Label	utPrecision = OUT_DEFAULT_PRECIS
10046DA7	. 6A 00	PUSH 0		Set = ANSI_CHARSET
10046DA9	. 6A 00	PUSH 0	Comment	StrikeOut = FALSE
10046DAB	. 6A 00	PUSH 0		Underline = FALSE
10046DAC	. 6A 00	PUSH 0	Breakpoint	Italic = FALSE
10046DAE	. 68 BC020000	PUSH 2BC	Hit trace	Weight = FW_BOLD
10046DB0	. 6A 00	PUSH 0	Run trace	Orientation = 0
10046DB2	. 6A 00	PUSH 0		Escapement = 0
10046DB4	. 8BF0	MOV ESI,EBX		n = 0
10046DB6	. 6A 10	PUSH 10		ht = 10 (16.)
10046DB8	. 8975 E0	MOV DWORD PTR SS:[EBP-20],ESI	Follow	Enter
10046DBA	. FF15 50100C10	CALL DWORD PTR DS:[<&GDI32.CreateFontW>]	New origin here	Ctrl+Gray *
10046DBD	. 8B7D 00	MOV EDI,DWORD PTR SS:[EBP-50]	Go to	ect
10046DBF	. 56	PUSH ESI	Follow in Dump	2.SelectObject
10046DC1	. 8B35 78100C10	MOV ESI,DWORD PTR DS:[<&GDI32.SelectObject>]		ect
10046DC3	. 8BD8	MOV EBX,EBX		ect
10046DC5	. 57	PUSH EDI		ect
10046DC7	. 895D 00	MOV DWORD PTR SS:[EBP-30],EBX	Search for	ectObject
10046DC9	. FFD6	CALL ESI	Find references to	ect
10046DCB	. 53	PUSH EBX	View	ectObject
10046DCE	. 57	PUSH EDI		ectObject
10046DCF	. 8945 00	MOV DWORD PTR SS:[EBP-50],EBX	Copy to executable	Selection
10046DD2	. FFD6	CALL ESI	Analysis	All modifications
10046DD4	. 68 FF000000	PUSH 0FF		
10046DD7	. 57	PUSH EDI		
10046DD8	. 8945 E8	MOV DWORD PTR SS:[EBP-10],EBX		
10046DDB	. FF15 54100C10	CALL DWORD PTR DS:[<&GDI32.SetTextColor>]		

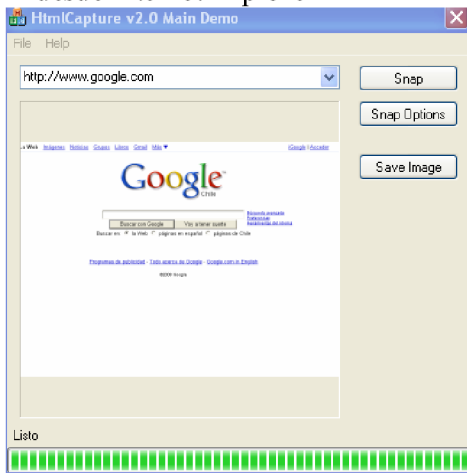
Evito que comienze la rutina

Y pff guardo el cambio  
Pruero



Waa cracked

Y desde Internet Explorer



Sip funciona

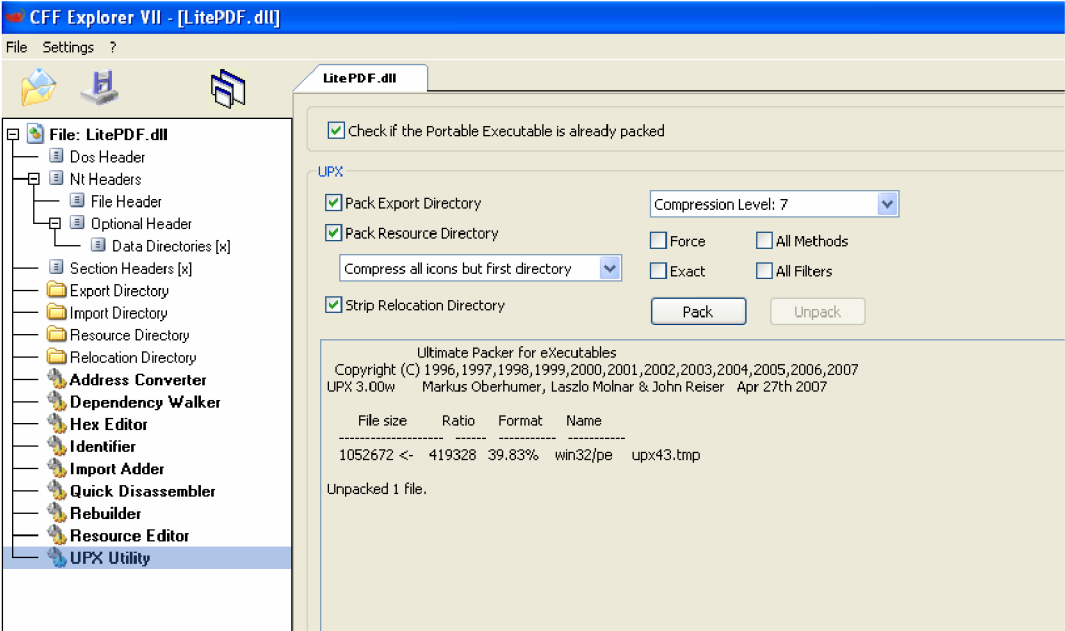
[Download HtmlCapture v2.0 NOW to Try it for FREE!](#)

[No functionality limitation except watermarks in the generated image for the unregistered version.](#)

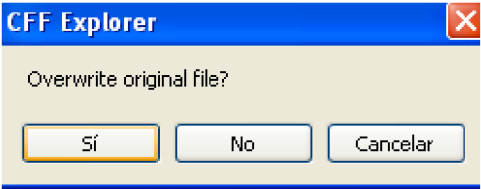
Ahora bien aremos un truco genial

Pero espero hacerlo en todos antes de comenzar este Apunte

Sigamos

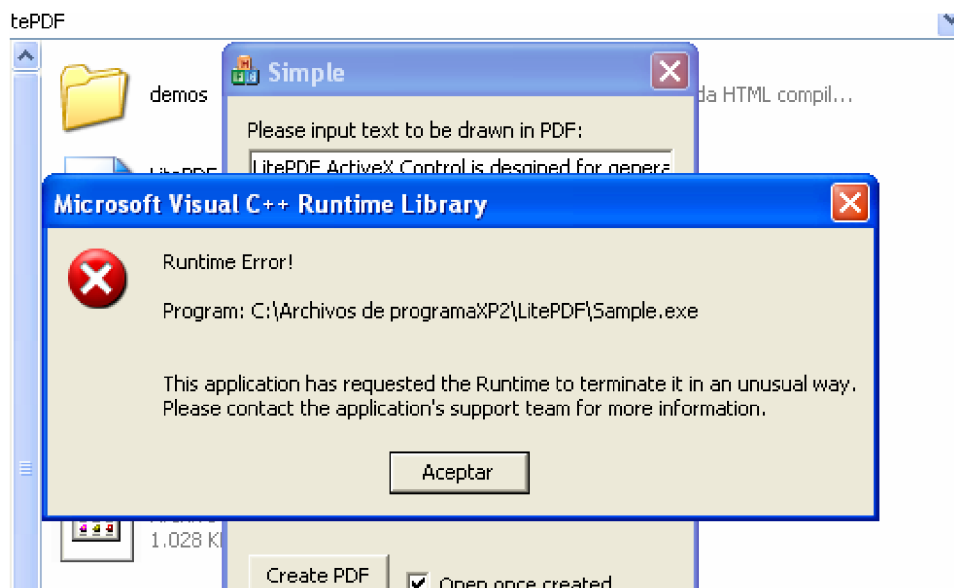


Descompresso, guardo



Voy a la referencia encontrada, con unregistered~

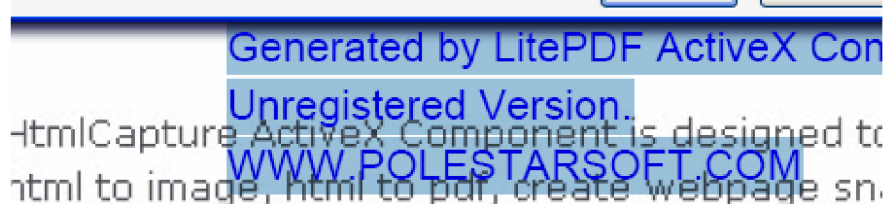
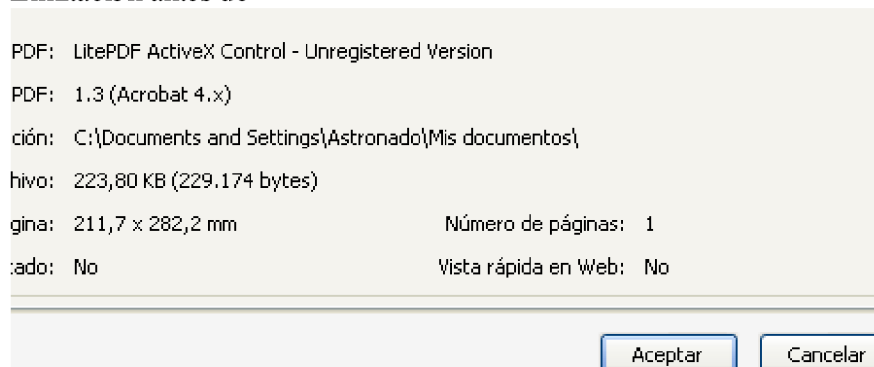
31FE7	66:8979 04	MOV WORD PTR DS:[ECX+4],DI	
31FEB	EA 15	JMP SHORT LitePDF.10032002	
31FED	6A 2E	PUSH 2E	
31FF4	68 20410B10	PUSH LitePDF.100B4120	UNICODE "LitePDF ActiveX Control - Unregistered Version"
31FF4	E8 4788FDFF	CALL LitePDF.1000A840	
31FF9	C745 FC 29000000	MOV DWORD PTR SS:[EBP-4],29	
32000	EB 13	JMP SHORT LitePDF.10032015	
32002	6A 17	PUSH 17	
32004	68 F0400B10	PUSH LitePDF.100B40F0	UNICODE "LitePDF ActiveX Control"
32009	E8 3288FDFF	CALL LitePDF.1000A840	
3200E	C745 FC 2A000000	MOV DWORD PTR SS:[EBP-4],2A	



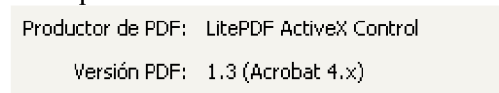
Eso paso porque estaba siendo ocupado? Sip, tenia abierto el pdf  
Jiji

Bueno eso paso realmente porque no es de los que reemplazan si esta el proceso  
ocupado~

Limitacion antes de



Y después

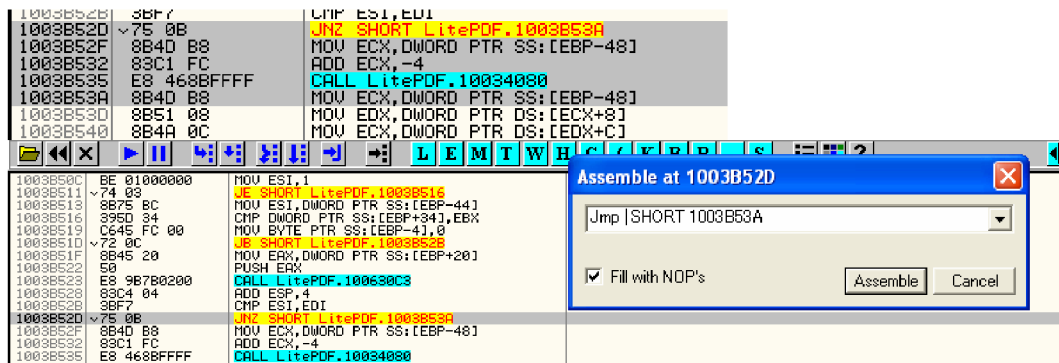
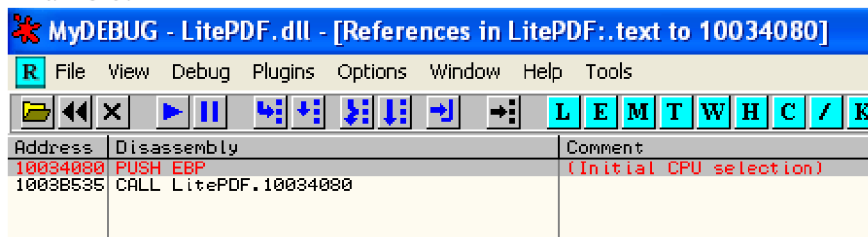


Aun falta el generated

Luego

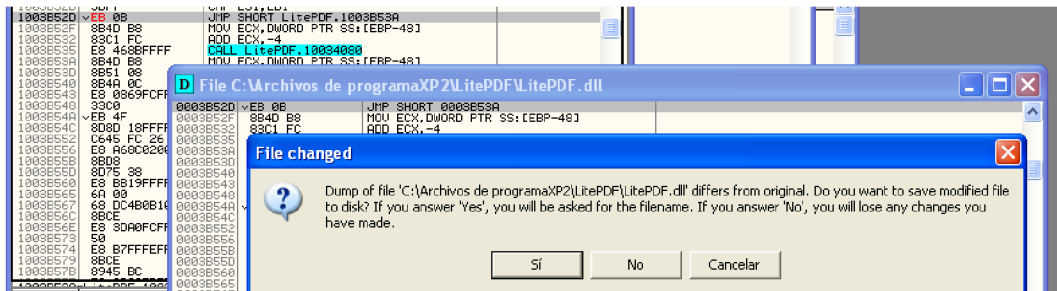
10034138	8979 18	MOV DWORD PTR DS:[ECX+18],EDI	
1003413B	8969 14	MOV DWORD PTR DS:[ECX+14],EBX	
1003413E	68 A0440B10	PUSH LitePDF.100B440B	Unicode "Generated by LitePDF ActiveX Control"
10034143	66 8959 04	MOV WORD PTR DS:[ECX+4],BX	
10034147	E8 F466F0FF	CALL LitePDF.100B0840	
1003414C	D945 C8	FLO DWORD PTR SS:[EBP-38]	
1003414F	DC25 A0440B10	FSUB QWORD PTR DS:[100B440B]	
10034155	884E 10	MOV ECX,DWORD PTR DS:[ESI+10]	
10034158	83EC 08	SUB ESP,8	
1003415B	D95D C8	FSTP QWORD PTR SS:[EBP-38]	
1003415E	D945 C4	FLO DWORD PTR SS:[EBP-3C]	
10034161	DC25 80440B10	FSUB QWORD PTR DS:[100B440B]	
10034167	D95D CC	FSTP QWORD PTR SS:[EBP-34]	
1003416A	D945 CC	FLO DWORD PTR SS:[EBP-34]	
1003416D	D95C24 04	FSTP QWORD PTR SS:[ESP+4]	
10034171	D945 C8	FLO DWORD PTR SS:[EBP-38]	
10034174	D91C24	FSTP QWORD PTR SS:[ESP]	
10034177	E8 E479F0FF	CALL LitePDF.100B0B60	
1003417C	83EC 1C	SUB ESP,1C	
1003417F	88CC	MOV ECX,ESP	
10034181	8965 CC	MOV DWORD PTR SS:[EBP-34],ESP	
10034184	6A 15	PUSH 15	
10034186	8979 18	MOV DWORD PTR DS:[ECX+18],EDI	
10034189	8969 14	MOV DWORD PTR DS:[ECX+14],EBX	
1003418C	68 60440B10	PUSH LitePDF.100B440B	Unicode "Unregistered Version."
10034191	66 8959 04	MOV WORD PTR DS:[ECX+4],BX	
10034195	E8 A666F0FF	CALL LitePDF.100B0840	
1003419A	D945 C4	FLO DWORD PTR SS:[EBP-3C]	
1003419D	DC25 60440B10	FSUB QWORD PTR DS:[100B440B]	
100341A3	884E 10	MOV ECX,DWORD PTR DS:[ESI+10]	
100341A6	83EC 08	SUB ESP,8	
100341A9	D95D CC	FSTP QWORD PTR SS:[EBP-34]	
100341AC	D945 CC	FLO DWORD PTR SS:[EBP-34]	
100341AF	D95C24 04	FSTP QWORD PTR SS:[ESP+4]	
100341B3	D945 C8	FLO DWORD PTR SS:[EBP-38]	
100341B6	D91C24	FSTP QWORD PTR SS:[ESP]	
1003407E	CC	INT3	
1003407F	CC	INT3	
10034080	55	PUSH EBP	
10034081	8BEC	MOV EBP,ESP	
10034083	6A FF	PUSH -1	
10034085	68 58EB0A10	PUSH LitePDF.100AEB58	
1003408A	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	
10034090	50	PUSH EAX	
10034091	83EC 68	SUB ESP,68	
10034094	A1 24130F10	MOV EAX,DWORD PTR DS:[100F1324]	
10034099	33C5	XOR EAX,EBP	
1003409B	8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	

Anализо ctrl+r

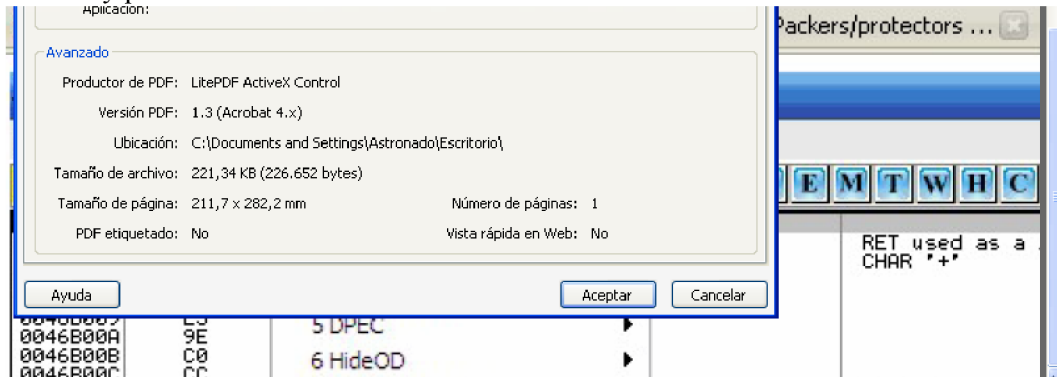


Si evito que llegue~ no hay watermark





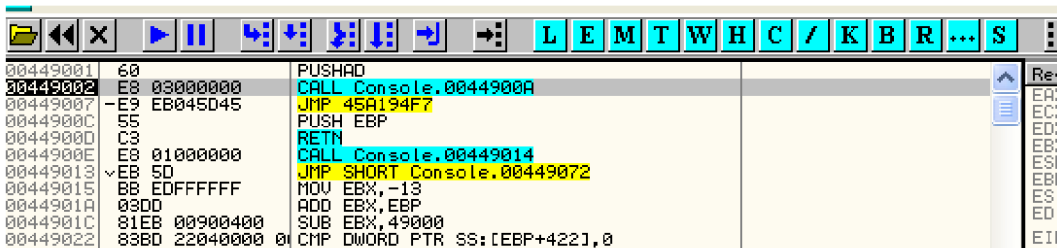
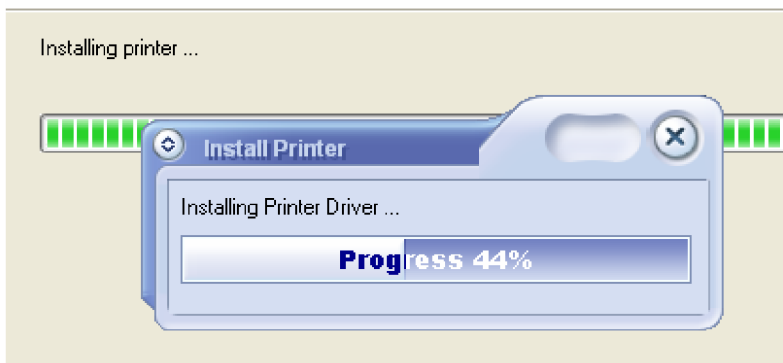
## Guardo y pruebo

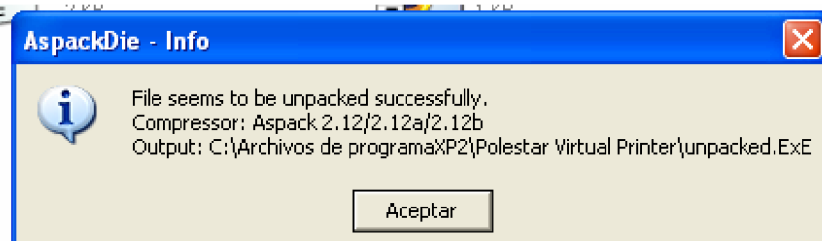


Sip, el pdf esta al final sin watermark

Jiji

Van 2 de 3





Asi que desempacado reviso y al parecer hay crc que no me abre

00402559	. 805424 0C	LEA EDX,DWORD PTR SS:[ESP+C]	
0040255E	. 8BCC	MOV ECX,ESP	
00402560	. 896424 14	MOV DWORD PTR SS:[ESP+14],ESP	
00402564	. 68 5CC44100	PUSH Console.0041C45C	Unicode "\console.exe.sf"
00402569	. 52	PUSH EDX	
0040256A	. 51	PUSH ECX	
0040256B	. E8 102B0100	CALL <JMP.&MFC42u.#925>	
00402570	. 51	PUSH ECX	
00402571	. 8D4C24 10	LEA ECX,DWORD PTR SS:[ESP+10]	
00402575	. 8BC4	MOV EAX,ESP	
00402577	. 896424 14	MOV DWORD PTR SS:[ESP+14],ESP	
0040257B	. 68 40C44100	PUSH Console.0041C440	Unicode "\console.exe"
00402580	. 51	PUSH ECX	
00402581	. 50	PUSH EAX	
00402582	. C68424 7C0300	MOV BYTE PTR SS:[ESP+37C],9	
0040258A	. E3 F12D0100	CALL <JMP.&MFC42u.#925>	
0040258F	. 8B9C24 700300	MOV BYTE PTR SS:[ESP+370],BL	
00402596	. E8 55280000	CALL Console.00404DF0	
0040259B	. 83C4 08	ADD ESP,8	
0040259E	. 3BC3	CMP EAX,EBX	
004025A0	. 0F84 31010000	JE Console.004026D7	
004025A6	. 51	PUSH ECX	
004025A7	. 8D424 0C	LEA EAX,DWORD PTR SS:[ESP+C]	
004025AB	. 8BD4	MOV EDX,ESP	
004025AD	. 896424 10	MOV DWORD PTR SS:[ESP+10],ESP	
004025B1	. 68 1CC44100	PUSH Console.0041C41C	Unicode "\distiller.exe.sf"
004025B6	. 50	PUSH EAX	
004025B7	. 52	PUSH EDX	
004025B8	. E8 C32A0100	CALL <JMP.&MFC42u.#925>	
004025BD	. 51	PUSH ECX	
004025BE	. 8D5424 10	LEA EDX,DWORD PTR SS:[ESP+10]	
004025C2	. 8BCC	MOV ECX,ESP	
004025C4	. 896424 18	MOV DWORD PTR SS:[ESP+18],ESP	
004025C8	. 68 FCC34100	PUSH Console.0041C3FC	Unicode "\distiller.exe"
004025CD	. 52	PUSH EDX	
004025CE	. 51	PUSH ECX	

Llegando de un momento a otro reviso y aca esta el probl...

00402596	. E8 55280000	CALL Console.00404DF0	
0040259B	. 83C4 08	ADD ESP,8	
0040259E	. 3BC3	CMP EAX,EBX	
004025A0	. 90	NOP	
004025A1	. 90	NOP	
004025A2	. 90	NOP	
004025A3	. 90	NOP	
004025A4	. 90	NOP	
004025A5	. 90	NOP	
004025A6	. 51	PUSH ECX	
004025A7	. 8D424 0C	LEA EAX,DWORD PTR SS:[ESP+C]	
004025AB	. 8BD4	MOV EDX,ESP	
004025AD	. 896424 10	MOV DWORD PTR SS:[ESP+10],ESP	
004025B1	. 68 1CC44100	PUSH Console.0041C41C	Unicode "\distiller.exe.sf"
004025B6	. 50	PUSH EAX	
004025B7	. 52	PUSH EDX	
004025B8	. E8 C32A0100	CALL <JMP.&MFC42u.#925>	
004025BD	. 51	PUSH ECX	
004025BE	. 8D5424 10	LEA EDX,DWORD PTR SS:[ESP+10]	
004025C2	. 8BCC	MOV ECX,ESP	
004025C4	. 896424 18	MOV DWORD PTR SS:[ESP+18],ESP	
004025C8	. 68 FCC34100	PUSH Console.0041C3FC	Unicode "\distiller.exe"
004025CD	. 52	PUSH EDX	
004025CE	. 51	PUSH ECX	
004025CF	. C68424 7C0300	MOV BYTE PTR SS:[ESP+37C],0A	
004025D7	. E8 A42A0100	CALL <JMP.&MFC42u.#925>	
004025DC	. 8B9C24 700300	MOV BYTE PTR SS:[ESP+370],BL	
004025E3	. E8 08280000	CALL Console.00404DF0	
004025E8	. 83C4 08	ADD ESP,8	
004025EB	. 3BC3	CMP EAX,EBX	
004025ED	. 90	NOP	
004025EE	. 90	NOP	
004025EF	. 90	NOP	
004025F0	. 90	NOP	
004025F1	. 90	NOP	
004025F2	. 90	NOP	
004025F3	. 53	PUSH EBX	

Nopeo antes que cambiar el push~

Péro tb podria haber ido al call y cambiarlo asi

00404DF0	33C0	NOP
00404DF2	80 01	XOR EAX,EAX
00404DF4	C3	MOV AL,1
00404DF5	90	RETN
00404DF6	90	NOP
00404DF7	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]
00404DFD	50	PUSH EAX
00404DFE	64:8925 000000	MOV DWORD PTR FS:[0],ESP
00404E05	83EC 48	SUB ESP,48
00404E08	53	PUSH EBX
00404E09	56	PUSH ESI
00404E0A	6A 01	PUSH 1
00404E0C	8D4C24 24	LEA ECX,DWORD PTR SS:[ESP+24]
00404E10	74424 5C 0100	MOV DWORD PTR SS:[ESP+5C],1

Porque la unica diferencia era si era 0, si daba 0 era mal, si era 1 era chico bueno

Ahora bien

**MyDEBUG - Distiller.exe - [MPU - main thread, module Distille]**

File View Debug Plugins Options Window Help Tools

Address Hex dump ASCII

00401254 . 8BD4 MOV EDI,ESP

00401256 . 896424 10 MOV DWORD PTR SS:[ESP+10],ESP

00401258 . 68 74A04600 PUSH Distille.0046A074

00401259 . 50 PUSH EAX

00401260 . 52 PUSH EDI

00401261 . C68424 F80000 MOV BYTE PTR SS:[ESP+F8],4

00401269 . E8 EEEF0300 CALL <JMP.&MFC42u.#925>

0040126E . C68424 EC0000 MOV BYTE PTR SS:[ESP+EC],2

00401276 . E8 1B340300 CALL Distille.004346E0

0040127B . 83C4 08 ADD ESP,8

0040127E . 85C0 TEST EAX,EAX

00401280 . 74 5D JE SHORT Distille.004012DF

00401282 . 51 PUSH ECX

00401283 . 8D5424 08 LEA EDI,DWORD PTR SS:[ESP+8]

00401287 . 8BCC MOV ECX,ESP

00401289 . 896424 0C MOV DWORD PTR SS:[ESP+C],ESP

00401292 . 68 50A04600 PUSH Distille.0046A050

00401293 . 52 PUSH EDI

00401294 . E8 C3EF0300 CALL <JMP.&MFC42u.#925>

00401299 . 51 PUSH ECX

0040129A . 8D4C24 0C LEA ECX,DWORD PTR SS:[ESP+C]

0040129E . 8BCC MOV EAX,ESP

004012A0 . 896424 14 MOV DWORD PTR SS:[ESP+14],ESP

004012A4 . 68 30A04600 PUSH Distille.0046A030

004012A9 . 51 PUSH ECX

004012AA . 50 PUSH EAX

004012AB . C68424 F80000 MOV BYTE PTR SS:[ESP+F8],5

004012B3 . E8 A4EF0300 CALL <JMP.&MFC42u.#925>

004012B8 . C68424 EC0000 MOV BYTE PTR SS:[ESP+EC],2

004012C0 . E8 1B340300 CALL Distille.004346E0

004012C5 . 83C4 08 ADD ESP,8

004012C8 . 85C0 TEST EAX,EAX

004012CA . 74 13 JE SHORT Distille.004012DF

004012CC . 8D4C24 10 LEA ECX,DWORD PTR SS:[ESP+10]

004012D0 . E8 DB1F0000 CALL Distille.004032B0

004012D5 . C68424 E40000 MOV BYTE PTR SS:[ESP+E4],7

004012D7 . E8 08 MOV EAX,ESP

004012D8 . C68424 E40000 MOV BYTE PTR SS:[ESP+E4],6

004012E7 . 8D5424 980000 LEA EDI,DWORD PTR SS:[ESP+98]

004012EE . E8 63EF0300 CALL <JMP.&MFC42u.#765>

004012F3 . 8D4C24 34 LEA ECX,DWORD PTR SS:[ESP+34]

004012F7 . C68424 E40000 MOV BYTE PTR SS:[ESP+E4],1

004012DF=Distille.004012DF

0012FE14 00000000

0012FE18 00000000


0012FE1C 00478988 Distille.00478

0012FE20 00383E08 UNICODE "C:\A

0012FE24 0015A000

Denuedo en el distiller

00401276	E8 65340300	CALL Distille.004346E0
0040127B	83C4 08	ADD ESP,8
0040127E	85C0	TEST EAX,EAX
00401280	90	NOP
00401281	90	NOP
00401282	51	PUSH ECX
00401283	8D5424 08	LEA EDI,DWORD PTR SS:[ESP+8]
00401287	8BCC	MOV ECX,ESP
00401289	896424 0C	MOV DWORD PTR SS:[ESP+C],ESP
00401292	68 50A04600	PUSH Distille.0046A050
00401293	52	PUSH EDI
00401294	E8 C3EF0300	CALL <JMP.&MFC42u.#925>
00401299	51	PUSH ECX
0040129A	8D4C24 0C	LEA ECX,DWORD PTR SS:[ESP+C]
0040129E	8BCC	MOV EAX,ESP
004012A0	896424 14	MOV DWORD PTR SS:[ESP+14],ESP
004012A4	68 30A04600	PUSH Distille.0046A030
004012A9	51	PUSH ECX
004012AA	50	PUSH EAX
004012AB	C68424 F80000	MOV BYTE PTR SS:[ESP+F8],5
004012B3	E8 A4EF0300	CALL <JMP.&MFC42u.#925>
004012B8	C68424 EC0000	MOV BYTE PTR SS:[ESP+EC],2
004012C0	E8 1B340300	CALL Distille.004346E0
004012C5	83C4 08	ADD ESP,8
004012C8	85C0	TEST EAX,EAX
004012CA	90	NOP
004012CC	8D4C24 10	LEA ECX,DWORD PTR SS:[ESP+10]
004012D0	E8 DB1F0000	CALL Distille.004032B0
004012D5	C68424 E40000	MOV BYTE PTR SS:[ESP+E4],7



Modificado el:

Aplicación: Polestar Virtual Printer

Astronado

Productor de PDF:

Versión PDF: 1.3 (Acrobat 4.x)

Ubicación: C:\Documents and Settings\Astronado\Mis documentos\

Tamaño de archivo: 164,94 KB (168.894 bytes)

Tamaño de página: 215 x 279 mm

Número de páginas: 1

PDF etiquetado: No

Vista rápida en Web: No

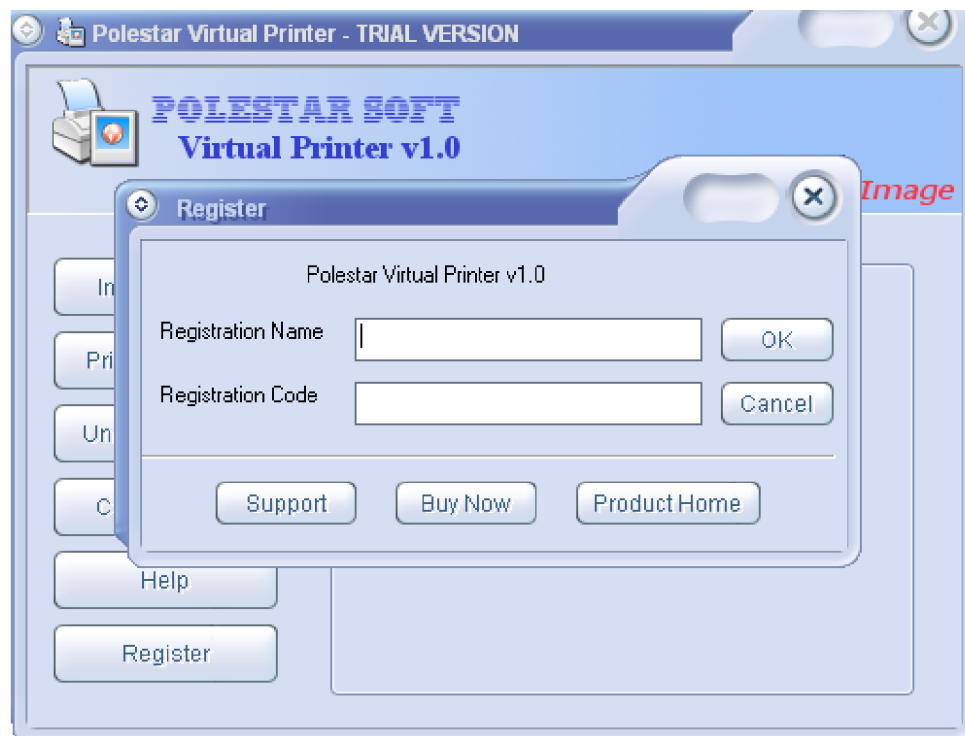
Vista rápida en Web

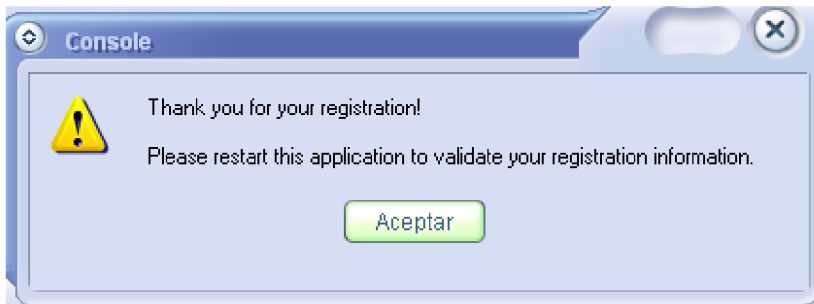
Aceptar

Cancelar

Polestar Virtual Printer v1.0  
Trial Version  
POLESTARSOFT.COM

0043388C	PUSH	Dist.ille.0047877C	UNICODE "SOFTWARE\POLESTARSOFT.COM\Virtual Printer\UserInfo"
0043389F	PUSH	Dist.ille.004787E8	UNICODE "UserName"
004338D5	PUSH	Dist.ille.004787D0	UNICODE "Key"
004338C9	PUSH	Dist.ille.004787D4	UNICODE "pass"
00433CE9	PUSH	Dist.ille.004787B8	UNICODE "LicenseCount"
00433DB9	MOV	EDI,Dist.ille.00478868	ASCII "149"
00433DEC	MOV	EDI,Dist.ille.00478864	ASCII "224"
00434003	PUSH	Dist.ille.00478866	UNICODE "XXXXXXXXXX"
0043417D	PUSH	Dist.ille.00478798	ASCII "hhc%28-wuq"





Y pff

Tenemos 30 dias mas pero bueno sigamos en el acto

Buscando la referencia free me doy cuenta de algo

0402C79	> 3206 00010000	UTF EAX,WORD PTR DS:[ESI+100]	
0402C79	> 75 17	JNE SHORT Console.00402C92	
0402C7B	> E8 302C0000	CALL Console.004058B0	
0402C80	> 85C0	TEST EAX,EAX	
0402C82	> 74 07	JE SHORT Console.00402C88	
0402C84	> 68 58C74100	PUSH Console.0041C758	UNICODE "About Polestar Virtual Printer."
0402C89	> EB 0C	JMP SHORT Console.00402C97	UNICODE "Polestar Virtual Printer is a FREE TRIAL shareware."
0402C8B	> 68 7CC44100	PUSH Console.0041C47C	
0402C90	> EB 05	JMP SHORT Console.00402C97	
0402C92	> 68 78D84100	PUSH Console.0041D878	
0402C97	> 8D8E 20010000	LEA ECX,DWORD PTR DS:[ESI+120]	
0402C9B	> E8 04220100	CALL Console.00402C97	

004058B0	81EC 0C020000	SUB ESP,20C
004058B6	53	PUSH EBX
004058B7	56	PUSH ESI
004058B8	57	PUSH EDI
004058B9	BF FCCC4100	MOV EDI,Console.0041CCFC
004058BE	83C9 FF	OR ECX,FFFFFFFF
004058C1	33C0	XOR EAX,EAX
004058C3	F2:AE	REPNE SCAS BYTE PTR ES:[EDI]
004058C5	F7D1	NOT ECX
004058C7	2BF9	SUB EDI,ECX
004058C9	8D5424 18	LEA EDX,DWORD PTR SS:[ESP+18]
004058CD	8BC1	MOV EAX,ECX
004058CF	8BF7	MOV ESI,EDI

En este call me decia el free trial algo

Bueno parcheo este que estaba mas o menos raro..

00408C9E	90	NOP	
00408CAF	90	NOP	
00408CB0	33C0	XOR EAX,EAX	
00408CB2	BA 01	MOV AL,1	
00408CB4	C3	RETN	
00408CB5	90	NOP	
00408CB6	90	NOP	
00408CB7	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	
00408CBD	50	PUSH EAX	
00408CBE	64:8925 00000000	MOV DWORD PTR FS:[0],ESP	
00408CC5	83EC 40	SUB ESP,40	
00408CC8	53	PUSH EBX	
00408CC9	56	PUSH ESI	
00408CCA	57	PUSH EDI	
00408CCB	6A 01	PUSH 1	
00408CCD	8D4C24 18	LEA ECX,DWORD PTR SS:[ESP+18]	
00408CD1	E8 8A4D0000	CALL Console.0040DA60	
00408CD6	33FF	XOR EDI,EDI	
00408CD8	6A 01	PUSH 1	
00408CDA	8D4C24 10	LEA ECX,DWORD PTR SS:[ESP+10]	
00408CDE	897C24 58	MOV DWORD PTR SS:[ESP+58],EDI	
00408CE2	E8 794D0000	CALL Console.0040DA60	
00408CE7	8D4424 24	LEA EAX,DWORD PTR SS:[ESP+24]	
00408CEB	68 1CCD4100	PUSH Console.0041CD1C	
00408CF0	50	PUSH EAX	
00408CF1	C64424 5C 01	MOV BYTE PTR SS:[ESP+5C],1	
00408CF6	E8 E5580000	CALL Console.0040E5E0	
00408CFB	8D4C24 24	LEA ECX,DWORD PTR SS:[ESP+24]	
00408CFF	68 90CD4100	PUSH Console.0041CD90	ASCII "23"

408cb2

Con eso tengo el about en vez de registred

Ahora me falta la nag

0040C0FF	90	NOP	
0040C100	53	PUSH EBX	
0040C101	56	PUSH ESI	
0040C102	57	PUSH EDI	
0040C103	8BF1	MOV ESI,ECX	
0040C105	6A 01	PUSH 1	
0040C107	E9 028E0000	CALL <JMP.&MFC42u.#6330>	
0040C10C	8D5E 64	LEA EBX,DWORD PTR DS:[ESI+64]	
0040C10F	8BCB	MOV ECX,EBX	
0040C111	E9 FC900000	CALL <JMP.&MFC42u.#6278>	
0040C116	8BCB	MOV ECX,EBX	
0040C118	E9 EF900000	CALL <JMP.&MFC42u.#6279>	
0040C11D	8D7E 60	LEA EDI,DWORD PTR DS:[ESI+60]	
0040C120	8BCF	MOV ECK,EDI	
0040C122	E9 EB900000	CALL <JMP.&MFC42u.#6278>	
0040C127	8BCF	MOV ECK,EDI	
0040C129	E9 DE900000	CALL <JMP.&MFC42u.#6279>	
0040C12E	8BCF	MOV ECK,EDI	
0040C130	E9 D1900000	CALL <JMP.&MFC42u.#4199>	
0040C135	8B1B	MOV EBX,DWORD PTR DS:[EBX]	
0040C137	8B43 F8	MOV EAX,DWORD PTR DS:[EBX-8]	
0040C13A	85C0	TEST EAX,EAX	
0040C13C	75 12	JNZ SHORT Console.0040C150	
0040C13E	6A 00	PUSH 0	
0040C140	6A 00	PUSH 0	
0040C142	68 C4D74100	PUSH Console.0041D7C4	UNICODE "Please enter your registration name!"
0040C147	E9 A8900000	CALL <JMP.&MFC42u.#1197>	
0040C14C	5F	POP EDI	
0040C14D	5E	POP ESI	
0040C14E	5B	POP EBX	
0040C14F	C3	RETN	
0040C150	8B3F	MOV EDI,DWORD PTR DS:[EDI]	
0040C152	8B47 F8	MOV EAX,DWORD PTR DS:[EDI-8]	
0040C155	85C0	TEST EAX,EAX	
0040C157	75 12	JNZ SHORT Console.0040C168	
0040C159	6A 00	PUSH 0	
0040C15B	6A 00	PUSH 0	
0040C15D	68 78D74100	PUSH Console.0041D778	UNICODE "Please enter your registration code!"
0040C162	E9 8D900000	CALL <JMP.&MFC42u.#1197>	

Al final de tracear termino aca

00404B37	85C0	TEST EAX,EAX	
00404B39	0F9FC1	SETG CL	
00404B3C	8BC1	MOV EAX,ECX	
00404B3E	C3	RETN	
00404B3F	90	NOP	
00404B40	55	PUSH EBP	
00404B41	8BEC	MOV EBP,ESP	

Esto determina si hay nag o no

Asi que parcheo

00404B35	33C9	XOR ECX,ECX	
00404B37	33C0	XOR EAX,EAX	
00404B39	8B 01	MOV AL,1	
00404B3B	90	NOP	
00404B3C	8BC1	MOV EAX,ECX	
00404B3E	C3	RETN	
00404B3F	90	NOP	
00404B40	55	PUSH EBP	
00404B41	8BEC	MOV EBP,ESP	

Pero la nag aparece igual

Wa

Elimino el recurso de registred y punto

Murio nag~

Ahora el watermark

POISONyBjēō - [Text strings referenced in Distille: text]		
File View Debug Plugins Options Window Help Tools		
L E M T W H C / K B R ... S		
Address	Disassembly	Text string
00401E4A	PUSH Distille.0046A104	Unicode "SOFTWARE\POLESTARSOFT.COM\Virtual Printer\Config"
00401E69	PUSH Distille.0046A0EC	Unicode "IngHorRes"
00401E88	PUSH Distille.0046A0D4	Unicode "IngVertRes"
00401F57	PUSH Distille.0046A238	Unicode "Creating ENF"
0040201E	PUSH Distille.0046A228	Unicode "%s%d%s"
00402057	PUSH Distille.0046A284	Unicode "Creating ENF Page"
004020C0	PUSH Distille.0046A1E8	ASCII "invalid vector<T> subscript"
004021EA	PUSH Distille.0046A2A0	Unicode ".jpg"
004021FD	PUSH Distille.0046A294	Unicode ".jpeg"
00402212	PUSH Distille.0046A274	Unicode "Creating Image"
00402266	PUSH Distille.0046A264	Unicode "image/"
0040233C	PUSH Distille.0046A254	Unicode "%s_d%s"
0040238F	PUSH Distille.0046A274	Unicode "Creating Image"
00402475	PUSH Distille.0046A1E8	ASCII "invalid vector<T> subscript"
004025E7	PUSH Distille.0046A2A8	Unicode "Creating page %d. %s"
00402C31	PUSH Distille.0046A2F4	Unicode "image/png"
00402C05	PUSH Distille.0046A308	Unicode "image/jpeg"
00402E94	PUSH Distille.0046A3A8	Unicode "\tinfo.img"
00402EFC	PUSH Distille.0046A39C	Unicode "Arial"
00402F5D	PUSH Distille.0046A360	Unicode "Polestar Virtual Printer v1.0"
00402F9D	PUSH Distille.0046A344	Unicode "Trial Version"
00402FD2	PUSH Distille.0046A320	Unicode "POLESTARSOFT.COM"
00403354	PUSH Distille.0046A44C	Unicode "PostView"
00403375	PUSH Distille.0046A4A0	Unicode "Open"
004036F1	PUSH Distille.0046A4E0	Unicode "SpoolDirectory"
0040374E	PUSH Distille.0046A4C8	Unicode "%s\%05d.sp1"
0040376A	PUSH Distille.0046A4C0	Unicode ".ps"
0040390E	PUSH Distille.0046A104	Unicode "SOFTWARE\POLESTARSOFT.COM\Virtual Printer\Config"
0040392D	PUSH Distille.0046A518	Unicode "PDFHorRes"
0040394C	PUSH Distille.0046A500	Unicode "PDFVertRes"
004039FC	PUSH Distille.0046A5E4	Unicode "Creating PDF"
00403A61	PUSH Distille.0046A4C0	Unicode ".ps"
00403A6D	PUSH Distille.0046A4C0	Unicode ".ps"

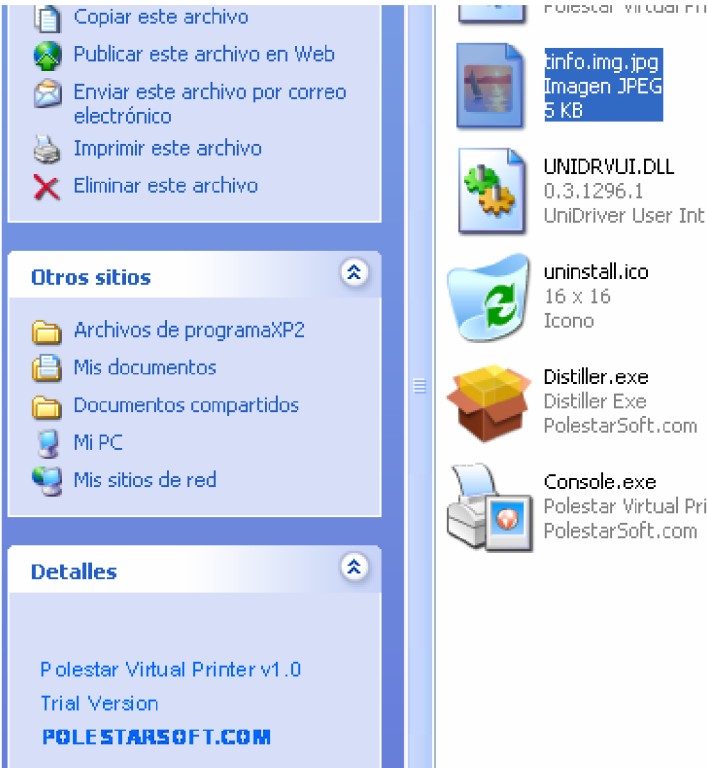
00402E98	804C24 00	LEA ECX, DWORD PTR SS:[ESP+8]	
00402E9C	89F0	MOV ESI, EAX	
00402EDE	E8 90D30300	CALL <JMP.&MFC42u.#800>	
00402E98	804C24 0C	LEA ECX, DWORD PTR SS:[ESP+C]	
00402EB7	C78424 840000	MOV DWORD PTR SS:[ESP+84], -1	
00402EC2	E8 89D30300	CALL <JMP.&MFC42u.#800>	
00402EC7	85F6	TEST ESI, ESI	
00402EC9	JE 5E010000	JMP Distille.0040302C	
00402EDF	8BB424 940000	MOV ESI, DWORD PTR SS:[ESP+94]	
00402ED6	B9 17000000	MOV ECX, 17	
00402EDB	33C0	XOR EAX, EAX	
00402EDD	007C24 20	LEA EDI, DWORD PTR SS:[ESP+20]	
00402EE1	F3AB	REP STOS DWORD PTR ES:[EDI]	
00402EE3	B8 859176AC	MOV EAX, AC769185	
00402EE8	53	PUSH EBX	
00402EE9	F7EE	INUL ESI	
00402EEB	0306	ADD EDX, ESI	
00402EED	55	PUSH EBP	
00402EEE	C1FA 06	SAR EDX, 6	
00402EF1	8BC2	MOV EAX, EDX	
00402EF3	804C24 44	LEA ECX, DWORD PTR SS:[ESP+44]	
00402EF7	C1E2 1F	SHR EAX, 1F	
00402EFA	03D0	ADD EDX, EAX	
00402EFC	68 9CA34600	PUSH Distille.0046A39C	
00402F01	51	PUSH ECX	
00402F02	C74424 40 900	MOV DWORD PTR SS:[ESP+40], 190	
00402F0A	895424 30	MOV DWORD PTR SS:[ESP+30], EDX	
00402F0E	FF15 24244400	CALL DWORD PTR DS:[<&MSVCRT.wcopy>]	src = "Arial" dest wcopy
00402F14	83C4 08	ADD ESP, 8	
00402F17	8D5424 28	LEA EDX, DWORD PTR SS:[ESP+28]	
00402F1B	C64424 3F 01	MOV BYTE PTR SS:[ESP+3F], 1	
00402F20	52	PUSH EDX	
00402F21	FF15 18204400	CALL DWORD PTR DS:[<&GDI32.CreateFontIndirectW>	LogFont CreateFontIndirectW
00402F27	8BAC24 940000	MOV EBP, DWORD PTR SS:[ESP+94]	
00402F2E	50	PUSH EAX	
00402F2F	55	PUSH EBP	hObject hDC
00402F30	FF15 98204400	CALL DWORD PTR DS:[<&GDI32.SelectObject>	SelectObject
00402F36	DB8424 9C0000	FILD DWORD PTR SS:[ESP+9C]	
00402F3D	DC00 F0264400	FIMUL QWORD PTR DS:[4426F0]	
00402F43	FA 26F6A300	CALL <JMP.&MSVCRT._ftello>	

El salto, debe ser jmp y listo

Pero como seguia

00402E65	83EC 74	SUB ESP, 74	
00402E68	56	PUSH ESI	
00402E69	57	PUSH EDI	
00402E6A	E8 214D0300	CALL Distille.00437B90	
00402E6F	85C0	TEST EAX, EAX	
00402E71	JE 5E010000	JMP Distille.00403094	
00402E77	8D4424 0C	LEA EAX, DWORD PTR SS:[ESP+C]	
00402E7B	50	PUSH EAX	
00402E7C	E8 9FF8FFFF	CALL Distille.00402720	
00402E81	83C4 04	ADD ESP, 4	
00402E84	68 A8A34600	PUSH Distille.0046A3A8	Unicode "\tinfo.img"
00402E89	8D4C24 0C	LEA ECX, DWORD PTR SS:[ESP+C]	
00402E8D	50	PUSH EAX	
00402E8E	51	PUSH ECX	
00402E8F	C78424 900000	MOV DWORD PTR SS:[ESP+90], 0	
00402E9A	E8 BDD30300	CALL <JMP.&MFC42u.#925>	
00402E9F	8B00	MOV EAX, DWORD PTR DS:[EAX]	FileName GetEnhMetaFileW
00402EA1	50	PUSH EAX	
00402EA2	FF15 1C204400	CALL DWORD PTR DS:[<&GDI32.GetEnhMetaFileW>	
00402EA8	8D4C24 08	LEA ECX, DWORD PTR SS:[ESP+8]	
00402EA9	50	MOV ESI, EAX	
00402EAE	E8 9DD30300	CALL <JMP.&MFC42u.#800>	
00402EB3	8D4C24 0C	LEA ECX, DWORD PTR SS:[ESP+C]	
00402EB7	C78424 840000	MOV DWORD PTR SS:[ESP+84], -1	
00402EC2	E8 89D30300	CALL <JMP.&MFC42u.#800>	
00402EC7	85F6	TEST ESI, ESI	
00402EC9	JE 5E010000	JMP Distille.0040302C	
00402EC9	90	NOP	
00402ECF	8BB424 940000	MOV ESI, DWORD PTR SS:[ESP+94]	
00402ED6	B9 17000000	MOV ECX, 17	

Supongo que es mas arriba



Me pongo a ver si esa.img es la causante , y sip esa es

Lo renombre a .jpg

Jiji

Ahora bien el call debe valer 1 para que el jnz sea como un jmp

00437B90	3300	XOR EAX,EAX	
00437B92	80 01	MOV AL,1	
00437B94	C3	RETN	
00437B95	90	NOP	
00437B96	90	NOP	
00437B97	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	
00437B9D	50	PUSH EAX	
00437B9E	64:8925 00000000	MOV DWORD PTR FS:[0],ESP	
00437BA5	83EC 40	SUB ESP,40	
00437BA8	53	PUSH EBX	
00437BA9	56	PUSH ESI	
00437BAA	57	PUSH EDI	
00437BAB	6A 01	PUSH 1	
00437BAD	8D4C24 18	LEA ECX,DWORD PTR SS:[ESP+18]	
00437BB1	E8 0A110000	CALL Distille.00438CC0	
00437BB6	33FF	XOR EDI,EDI	
00437BB8	6A 01	PUSH 1	
00437BBA	8D4C24 10	LEA ECX,DWORD PTR SS:[ESP+10]	
00437BBE	897C24 58	MOV DWORD PTR SS:[ESP+58],EDI	
00437BC2	E8 F9100000	CALL Distille.00438CC0	
00437BC7	8D4424 24	LEA EAX,DWORD PTR SS:[ESP+24]	
00437BCB	68 94884700	PUSH Distille.00478894	
00437BD0	50	PUSH EAX	
00437BD1	C64424 5C 01	MOV BYTE PTR SS:[ESP+5C],1	
00437BD6	E8 651C0000	CALL Distille.00439840	
00437BD8	8D4C24 24	LEA ECX,DWORD PTR SS:[ESP+24]	
00437BDF	68 08894700	PUSH Distille.00478908	
00437BE4	51	PUSH ECX	ASCII "23"
00437BE5	C64424 64 02	MOV BYTE PTR SS:[ESP+64],2	
00437BEA	E8 511C0000	CALL Distille.00439840	
00437BEF	83C4 10	ADD ESP,10	
00437BF0	50	PUSH EAX	

Y pff

Sumo los valores base



329.85 US Dollar(s) = **145371** Chilean Peso(s)  
1 CLP = 0.00226901 USD  
1 USD = 440.72 CLP

Y eso fue todo  
Eso ahorramos hoy.

#### Conclusiones

El tercer programa que es mas barato, da menos líos que los otros dos.

Si hubiera que pagar por alguno, sería el tercero.

Apuro mafo

Úsalo por los 30 días y después desinstálalo

Visión es el arte de ver las cosas invisibles. Jonathan Swift (1667-1745); político y escritor irlandés

Saber es acordarse. Aristóteles (384-322 a. C.); filósofo griego .

Comprender es el principio de aprobar Baruch Benedict Spinoza (1632-1677); filósofo holandés .