

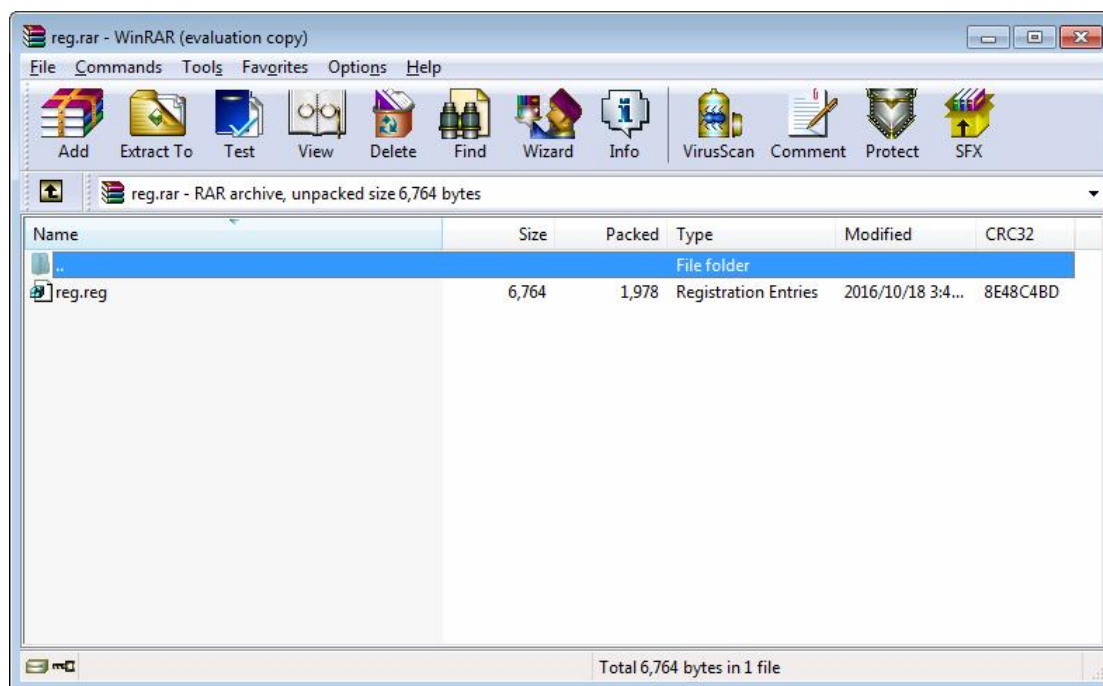
سری آموزش های R4NDOM-فارسی

قسمت 15- استفاده از Call Stack

در این قسمت ما محدودیت Nag Screen یک برنامه واقعی (WinRAR فمیه شده) را خواهیم برداشت. هدف انتخاب این برنامه این بود که هم نسخه ی کرک شده ی آن به وفور در اینترنت موجود است و همچنین با کم ترین آسیب به سافتار برنامه آن را بهینه کنیم (برای مصرف خودمان) به هر حال توصیه ی همیشگی مبنی بر حمایت از توسعه دهنده را گوشزد میکنم. البته این محدودیت را به روش جدیدی رفع خواهیم کرد، نکته ی قابل ذکر اینست که اگر سیستم عامل مورد استفاده ی شما WINDOWS 7 64 Bit (مثله من) است، تمامی نسخه های Olly 1.10 حتی نسخه ی R4NDOM در قسمتی که میفاهم آن آموزش دهم (تکنیک Call Stack) ناکارآمد هستند. پیشنهاد من این است که از نسخه ی Olly 2.0 فقط برای اجرای (ترفند) و بدست آوردن آدرس صحیح استفاده کنید. و دوباره به همان نسخه ی Olly 1.10 برای ادامه ی کار باز خواهیم گشت. یا اگر دوست دارید ادامه کار را با همان نسخه ی Olly 2.0 ادامه دهید. که انتخاب بسیار خوبی هم هست به غیر از ویژگی های جدیدش، به قول معروف امتحان خود را هم در سیستم های 64 بیتی پس داده است.

بررسی برنامه

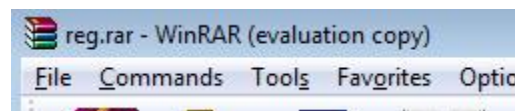
وقتی برنامه را مورد بررسی قرار میدهم متوجه میشویم که بعد از 40 روز (نویسنده در دست اندازه ی زمان روزه داری مضرت مسیح در بیابان) Nag Screen ظاهر میشود. (شک نکنید ☺) شما دو راه دارید یا 40 روز و شب صبر کنید تا Nag نمایش داده شود یا اینکه ساعت سیستم خود را 41 روز به جلو بیاورید و بعد از انجام آموزش دوباره به عقب بازگردانید.



و بعد از 40 روز :



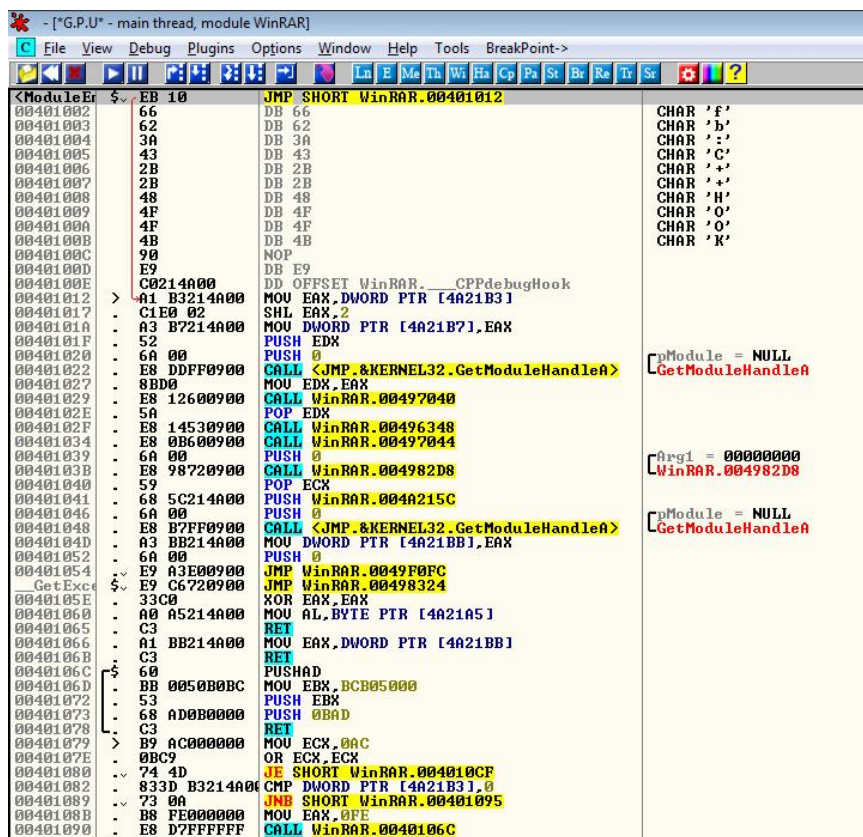
بعد از 40 روز هر موقع که winrar باز شود این Nag Screen ظاهر میشود و بسیار هم آزار دهنده هست، همچنین در قسمت بالای پنجره ی اصلی عبارت "evaluation copy" را میتوان دید:



من میخواهم دو روش برای رسیدن به قسمت مورد نظر نشان دهم

اولین راه:

برنامه را درون Olly باز کنید:



و سپس برنامه را تمت دیباگر اجرا کنید تا Nag Screen ظاهر شود، قبل از آنکه آن را ببندید بروی Pause کلیک کنید تا Olly موقتاً متوقف شود:



حالا ما میخواهیم بدانیم که این Nag از کجا آمده است. البته میتوان از تکنیک های intermodular calls و جستجوی رشته ها بهره برد اما به شما قول میدهم که به اندازه ی این تکنیک نمیتواند مفید باشد. همینطور از این تکنیک میتوان برای بسیاری از برنامه ها به کاربرد متی زمانی که رشته ای وجود ندارد استفاده کرد، گذشته از این ، این تکنیک بسیار سریعتر خواهد بود

Call Stack

اکثر کامپایلرها برای فراخوانی و برگشت زیربرنامه فراخوانی پشته (call stack) را پیاده سازی می کنند . Call stack یا run-time stack یک پشته است که اطلاعاتی درباره زیربرنامه فعال یک برنامه را نگهداری می کند. زیربرنامه فعال زیربرنامه ای است که فراخوانی شده است اما هنوز اجرائش تمام نشده است.

OllyDBG هم با ردیابی فراخوانی فعال محل آن را نمایش میدهد همچنین سعی میکند که آگومان های انتقال داده شده ی مربوط به تابع را نمایش دهد تمامی این فرایندها روند طبیعی Stack است و آن را میتوان در پنجره ی Stack (پایین سمت راست OllyDBG) دید، اما یادتان باشد ollydbg در این زمینه کامل نیست ، (Call Stack) و بالطبع شما هم نمیتوانید از تمام چیزهایی که درون این پنجره هستند استفاده کنید، از طرفی خیلی از اوقات هم این پنجره هنگام مهندسی معکوس برنامه های VB فالی هست (برنامه های vb توابع را مانند زبان های برنامه نویسی واقعی فراخوانی نمیکنند) ، برای نمایش پنجره ی Call Stack کلید "St" مفف Stack در نسخه ی R4NDOM یا اگر از نسخه ی اورجینال استفاده میکنید دکمه ی 'K' را بفشارید در زبان مادری نویسنده دیباگر احتمالاً با K شروع میشود :



بعد از فشردن :

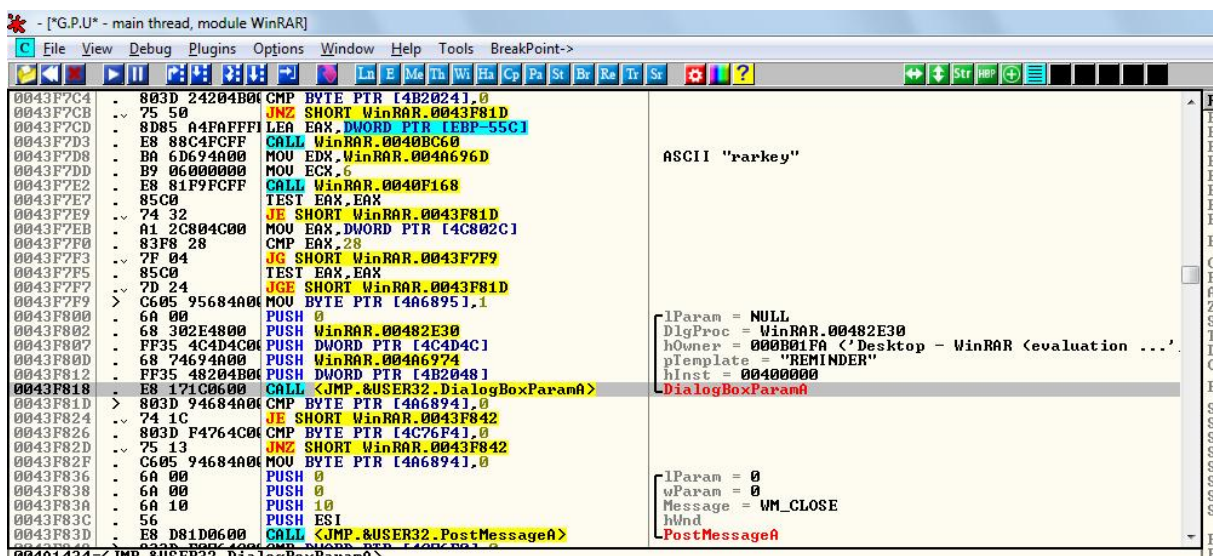
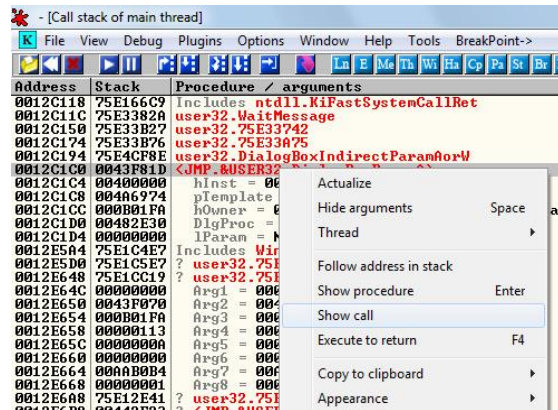
Address	Stack	Procedure / arguments	Called from	Frame
0012C118	75E166C9	Includes ntdll.KiFastSystemCallRet	user32.75E166C7	0012C14C
0012C11C	75E3382A	user32.WaitMessage	user32.75E33825	0012C14C
0012C150	75E33B27	user32.75E33742	user32.75E33B22	0012C14C
0012C174	75E33B76	user32.75E33A75	user32.75E33B71	0012C170
0012C194	75E4CF8E	user32.DialogBoxIndirectParamAorW	user32.75E4CF89	0012C190
0012C1C0	0043F81D	<JMP.&USER32.DialogBoxParamA>	WinRAR.0043F818	0012C1BC
0012C1C4	00400000	hInst = 00400000		
0012C1C8	004A6974	pTemplate = "REMINDER"		
0012C1CC	000B01FA	hOwner = 000B01FA ("Desktop - WinRAR (evaluation ...)		
0012C1D0	00482E30	DlgProc = WinRAR.00482E30		
0012C1D4	00000000	lParam = NULL		
0012E5A4	75E1C4E7	Includes WinRAR.0043F81D	user32.75E1C4E4	0012E5A0
0012E5D0	75E1C5E7	? user32.75E1C4C4	user32.75E1C5E2	0012E5CC
0012E648	75E1CC19	? user32.75E1C534	user32.75E1CC14	0012E644
0012E6A8	75E12E41	? user32.75E1CB33	user32.75E12E3C	0012E6A4
0012E6B8	00442F23	? <JMP.&USER32.DispatchMessageA>	WinRAR.00442F1E	0012E6B4
0012E6BC	0012E6C0	pMsg = WM_TIMER hw = B01FA ("Desktop - WinRAR (evaluation ...)		
0012E6EC	00442B34	? WinRAR.00442C44	WinRAR.00442B2F	

چند نکته در تصویر بالا قابل ذکر است، اول اینکه در ابتدای اولین Call که در بالا میبینیم عبارت 'Includes' درج شده که به معنی درگیر بودن دستورالعمل به وسیله ی این Call است، ولی Oly دقیقاً نمیتواند پگونگی آن را مشخص کند، در این مثال ما در ابتدا تابع ntdll را میبینیم، همینطور در پاینتر تعدادی تابع user32 را میبینیم. که تابع DialogBoxParamA و DialogBoxIndirectParamAorW با آرگومان های خود فراخوانی شده اند، و همینطور در پاینتر تعدادی Call دیگر مربوط به user32 داریم و در خط آخر winrar در آدرس 00442C44 تابع DispatchMessageA فراخوانی شده همچنین تابع DialogBoxParamA در User32 مسئول نمایش دیاالوگ باکس و متن "evaluation" "copy است و پس از نمایش دیاالوگ باکس و متن مورد نظر منتظر ورودی کاربر با استفاده از تابع WaitMessage میشود:

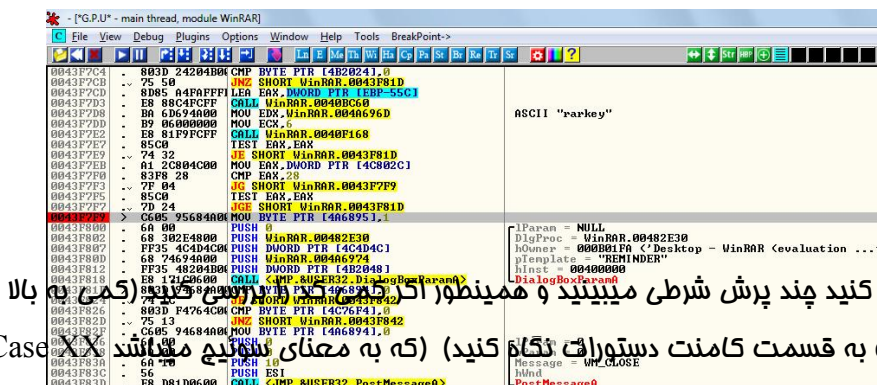
Address	Stack	Procedure / arguments	Called from	Frame
0012C118	75E166C9	Includes ntdll.KiFastSystemCallRet	user32.75E166C7	0012C14C
0012C11C	75E3382A	user32.WaitMessage	user32.75E33825	0012C14C
0012C150	75E33B27	user32.75E33742	user32.75E33B22	0012C14C
0012C174	75E33B76	user32.75E33A75	user32.75E33B71	0012C170
0012C194	75E4CF8E	user32.DialogBoxIndirectParamAorW	user32.75E4CF89	0012C190
0012C1C0	0043F81D	<JMP.&USER32.DialogBoxParamA>	WinRAR.0043F818	0012C1BC
0012C1C4	00400000	hInst = 00400000		
0012C1C8	004A6974	pTemplate = "REMINDER"		
0012C1CC	000B01FA	hOwner = 000B01FA ("Desktop - WinRAR (evaluation ...)		
0012C1D0	00482E30	DlgProc = WinRAR.00482E30		
0012C1D4	00000000	lParam = NULL		
0012E5A4	75E1C4E7	Includes WinRAR.0043F81D	user32.75E1C4E4	0012E5A0
0012E5D0	75E1C5E7	? user32.75E1C4C4	user32.75E1C5E2	0012E5CC
0012E648	75E1CC19	? user32.75E1C534	user32.75E1CC14	0012E644
0012E6A8	75E12E41	? user32.75E1CB33	user32.75E12E3C	0012E6A4
0012E6B8	00442F23	? <JMP.&USER32.DispatchMessageA>	WinRAR.00442F1E	0012E6B4
0012E6BC	0012E6C0	pMsg = WM_TIMER hw = B01FA ("Desktop - WinRAR (evaluation ...)		
0012E6EC	00442B34	? WinRAR.00442C44	WinRAR.00442B2F	

مهمترین چیز در این پنجره فراخوانی دیاالوگ باکس و محل آن در برنامه ما است، معمولاً وقتی از call stack استفاده میکنیم، از بالای پنجره ی Stack شروع میکنیم، به عبارت دیگر از اولین آیتم شروع

میکنیم، علت آن این است که تابعی را بیابیم که در برنامه (کد سکشن) فراخوانی شده باشد، اگر به هردلیلی موفق نشدید، آیتم های بعدی را چک کنید، تا به کد سکشن برنامه ارجاع داده شوید، و پس از ارجاع به کد سکشن، کمی کد را بررسی کنید و مطمئن شوید که آیا تابع مورد نظر در آنجا فراخوانی شده یا نه. ما در اینجا تابع DialogBoxParamA را مورد بررسی قرار میدهیم بروی آن راست کلیک کنید و از منوی باز شده show call را انتخاب کنید تا به محل آن ارجاع داده شویم:



بله، به تابع مورد نظر ارجاع شده ایم حالا من یک BP در ابتدای ساخته شدن و نمایش دیاپوگ باکس میگذارم:



اگر به بالا نگاه کنید چند پرش شرطی میبینید و همینطور اگر به پایین نگاه کنید (که به معنای سورس میباشند "Case") اسکرول کنید و به قسمت کامنت دستورات نگاه کنید

(WM_Something) را فواید دید در آدرس 0043F0A4 و xx در قالب مد هگزا است به معنای

شماره ی case

0043F766	BA 60694A00	MOV EDX,WinRAR.004A6960	ASCII "HELPHelpMenu"
0043F76B	33C9	XOR ECK,ECK	
0043F76D	8BC6	MOV EAX,ESI	
0043F76F	E8 A8470200	CALL WinRAR.00463F1C	
0043F774	E9 5A140000	JMP WinRAR.00440BD3	
0043F779	8B45 10	MOV EAX,DWORD PTR [EBP+10]	Case 7B <WM_CONTEXTMENU> of switch 0043F0A4
0043F77C	3B05 604D4C00	CMP EAX,DWORD PTR [4C4D60]	
0043F782	0F85 4B140000	JNZ WinRAR.00440BD3	
0043F788	B8 604D4C00	MOV EAX,WinRAR.004C4D60	
0043F78D	E8 4ACD0100	CALL WinRAR.0045C4D0	
0043F792	E9 3C140000	JMP WinRAR.00440BD3	
0043F797	833D F0764C00	CMP DWORD PTR [4C76F0],0	Case 113 <WM_TIMER> of switch 0043F0A4
0043F79E	75 7D	JNZ SHORT WinRAR.0043F81D	
0043F7A0	8D95 A4FAFFFI	LEA EDX,DWORD PTR [EBP-55C]	
0043F7A6	B8 A85A4C00	MOV EAX,WinRAR.004C5A88	
0043F7AB	33C9	XOR ECK,ECK	
0043F7AD	E8 2E7A0100	CALL WinRAR.004571E0	
0043F7B2	803D 95684A00	CMP BYTE PTR [4A6895],0	
0043F7B9	75 62	JNZ SHORT WinRAR.0043F81D	
0043F7BB	803D 8C854C00	CMP BYTE PTR [4C858C],0	
0043F7C2	75 59	JNZ SHORT WinRAR.0043F81D	
0043F7C4	803D 24204B00	CMP BYTE PTR [4B2041],0	
0043F7CB	75 50	JNZ SHORT WinRAR.0043F81D	
0043F7CD	8D85 A4FAFFFI	LEA EAX,DWORD PTR [EBP-55C]	
0043F7D3	E8 88C4FCFF	CALL WinRAR.0040BC60	
0043F7D8	BA 6D694A00	MOV EDX,WinRAR.004A696D	
0043F7DD	B9 06000000	MOV ECK,6	ASCII "rarkey"
0043F7E2	E8 81F9FCFF	CALL WinRAR.0040F168	
0043F7E7	85C0	TEST EAX,EAX	
0043F7E9	74 32	JE SHORT WinRAR.0043F81D	
0043F7EB	A1 2C804C00	MOV EAX,DWORD PTR [4C802C]	
0043F7F0	83F8 28	CMP EAX,28	
0043F7F3	7F 04	JG SHORT WinRAR.0043F7F9	
0043F7F5	85C0	TEST EAX,EAX	
0043F7F7	7D 24	JGE SHORT WinRAR.0043F81D	
0043F800	C605 95684A00	MOV BYTE PTR [4A6895],1	
0043F802	6A 00	PUSH 0	
0043F807	68 302E4800	PUSH WinRAR.00482E30	
0043F807	FF35 4C4D4C00	PUSH DWORD PTR [4C4D4C]	
0043F80D	68 74694A00	PUSH WinRAR.004A6974	
0043F812	FF35 48204B00	PUSH DWORD PTR [4B204B]	

دیباگر وضعیت سوئیچ ها را به ما نشان میدهد اگر در سکش جاری اسکرول به بالا کنید فواید دید که تعداد این سوئیچ ها بقدر زیاد است ،اگر با برنامه نویسی ویندوز آشنا باشید درکش برای شما بسیار روان فواید بود اما اگر هیچ تجربه ای ندارید نگران نباشید در آموزش ها بعدی جزئیات بیشتری در قست نمایش پنجره ها فواید آموخت،اما الان ما فقط علاقه مند به سوئیچ نمایش پنجره nag هستیم :

0043F766	BA 60694A00	MOV EDX,WinRAR.004A6960	ASCII "HELPHelpMenu"
0043F76B	33C9	XOR ECK,ECK	
0043F76D	8BC6	MOV EAX,ESI	
0043F76F	E8 A8470200	CALL WinRAR.00463F1C	
0043F774	E9 5A140000	JMP WinRAR.00440BD3	
0043F779	8B45 10	MOV EAX,DWORD PTR [EBP+10]	Case 7B <WM_CONTEXTMENU> of switch 0043F0A4
0043F77C	3B05 604D4C00	CMP EAX,DWORD PTR [4C4D60]	
0043F782	0F85 4B140000	JNZ WinRAR.00440BD3	
0043F788	B8 604D4C00	MOV EAX,WinRAR.004C4D60	
0043F78D	E8 4ACD0100	CALL WinRAR.0045C4D0	
0043F792	E9 3C140000	JMP WinRAR.00440BD3	
0043F797	833D F0764C00	CMP DWORD PTR [4C76F0],0	Case 113 <WM_TIMER> of switch 0043F0A4
0043F79E	75 7D	JNZ SHORT WinRAR.0043F81D	
0043F7A0	8D95 A4FAFFFI	LEA EDX,DWORD PTR [EBP-55C]	
0043F7A6	B8 A85A4C00	MOV EAX,WinRAR.004C5A88	
0043F7AB	33C9	XOR ECK,ECK	
0043F7AD	E8 2E7A0100	CALL WinRAR.004571E0	
0043F7B2	803D 95684A00	CMP BYTE PTR [4A6895],0	
0043F7B9	75 62	JNZ SHORT WinRAR.0043F81D	
0043F7BB	803D 8C854C00	CMP BYTE PTR [4C858C],0	
0043F7C2	75 59	JNZ SHORT WinRAR.0043F81D	
0043F7C4	803D 24204B00	CMP BYTE PTR [4B2041],0	
0043F7CB	75 50	JNZ SHORT WinRAR.0043F81D	
0043F7CD	8D85 A4FAFFFI	LEA EAX,DWORD PTR [EBP-55C]	
0043F7D3	E8 88C4FCFF	CALL WinRAR.0040BC60	
0043F7D8	BA 6D694A00	MOV EDX,WinRAR.004A696D	
0043F7DD	B9 06000000	MOV ECK,6	ASCII "rarkey"
0043F7E2	E8 81F9FCFF	CALL WinRAR.0040F168	
0043F7E7	85C0	TEST EAX,EAX	
0043F7E9	74 32	JE SHORT WinRAR.0043F81D	
0043F7EB	A1 2C804C00	MOV EAX,DWORD PTR [4C802C]	
0043F7F0	83F8 28	CMP EAX,28	
0043F7F3	7F 04	JG SHORT WinRAR.0043F7F9	
0043F7F5	85C0	TEST EAX,EAX	
0043F7F7	7D 24	JGE SHORT WinRAR.0043F81D	
0043F800	C605 95684A00	MOV BYTE PTR [4A6895],1	
0043F802	6A 00	PUSH 0	
0043F807	68 302E4800	PUSH WinRAR.00482E30	
0043F807	FF35 4C4D4C00	PUSH DWORD PTR [4C4D4C]	
0043F80D	68 74694A00	PUSH WinRAR.004A6974	
0043F812	FF35 48204B00	PUSH DWORD PTR [4B204B]	

DS:[004C76F0]=00000000
Jump from 0043F177

همان طور که میدانید قسمت WM_TIMER بازگو کننده ی فیلوی چیزهاست درواقع مشخص میشود که چرا مدام این پنجره(NAG) نمایش داده میشود و اینکه اگر تایمر خاموش شود چه اتفاقی خواهد افتاد ،مختصرا خواهیم دید و همینطور که میبینید بعد از نمایش دیالوگ باکس چند پرش شرطی داریم :

0043F7F7	> 7D 24	JGE SHORT WinRAR.0043F81D	
0043F7F9	> C605 95684A00	MOV BYTE PTR [4A6895],1	
0043F800	> 6A 00	PUSH 0	
0043F802	> 68 302E4800	PUSH WinRAR.00482E30	
0043F807	> FF35 4C4D4C00	PUSH DWORD PTR [4C4D4C]	
0043F80D	> 68 74694A00	PUSH WinRAR.004A6974	
0043F812	> FF35 48204B00	PUSH DWORD PTR [4B204B]	
0043F818	> E8 17C06000	CALL <JMP,USER32,DialogBoxParamA>	
0043F81D	> 803D 94684A00	CMP BYTE PTR [4A6894],0	
0043F824	> 74 1C	JE SHORT WinRAR.0043F842	
0043F826	> 803D F4764C00	CMP BYTE PTR [4C76F4],0	
0043F82D	> 75 13	JNZ SHORT WinRAR.0043F842	
0043F82F	> C605 94684A00	MOV BYTE PTR [4A6894],0	

```

iParam = NULL
DlgProc = WinRAR.00482E30
hOwner = 000B01FA <'Desktop - WinRAR (evaluation ...'
pTemplate = "REMINDER"
hInst = 00400000
DialogBoxParamA

```

این پرش ها بسته به اینکه کاربر چه کاری میکنند انتخاب و اجرا میشوند مثلا اگر کاربر بروی close کلیک کند ،پنجره بسته میشود

خب برمیگردیم به قسمت مورد نظر یعنی ابتدای سوئیچ تایمر در آدرس :43F797 یک BP بگذارید (اگر قبلا نگذاشته اید):

0043F79C	> 3B05 604D4C00	CMPL DWORD PTR DS:[4C4D4C],0	
0043F7B2	> 0F85 4B140000	JNZ WinRAR.004408D3	
0043F7B8	> B8 604D4C00	MOV EAX,WinRAR.004C4D68	
0043F7BD	> E8 4AC00100	CALL WinRAR.0045C4DC	
0043F7C2	> E9 3C140000	JMP WinRAR.00444B03	
0043F7C8	> 83D0 F0764C00 00	CMPL DWORD PTR DS:[4C76F0],0	
0043F79E	> 75 7D	JNZ SHORT WinRAR.0043F81D	
0043F7A0	> 8D95 A4FAFFFF	LEA EDI,DWORD PTR SS:[EBP-55C]	
0043F7A6	> B8 A85A4C00	MOV EAX,WinRAR.004C5A48	
0043F7AB	> 33C9	XOR ECX,ECX	
0043F7AD	> E8 2E7A0100	CALL WinRAR.004571E0	
0043F7B2	> 803D 95684A00 00	CMPL BYTE PTR DS:[4A6895],0	
0043F7B9	> 75 62	JNZ SHORT WinRAR.0043F81D	
0043F7BB	> 803D 8C854C00 00	CMPL BYTE PTR DS:[4C854C],0	
0043F7C2	> 75 59	JNZ SHORT WinRAR.0043F81D	
0043F7C4	> 803D 24204B00 00	CMPL BYTE PTR DS:[4B204B],0	
0043F7C8	> 75 50	JNZ SHORT WinRAR.0043F81D	
0043F7CD	> 8D95 A4FAFFFF	LEA EDI,DWORD PTR SS:[EBP-55C]	
0043F7D3	> E8 88C4FCFF	CALL WinRAR.0040BC60	
0043F7D8	> B8 6D694A00	MOV EAX,WinRAR.004A696D	
0043F7DD	> E9 06000000	MOV ECX,6	
0043F7E2	> E8 91F9FCFF	CALL WinRAR.0040F168	
0043F7E7	> 95C0	TEST EAX,EAX	
0043F7E9	> 74 32	JE SHORT WinRAR.0043F81D	
0043F7EB	> A1 2C804C00	MOV EAX,DWORD PTR DS:[4C802C]	
0043F7F0	> 83F8 28	CMPL EAX,28	
0043F7F3	> 7F 04	JG SHORT WinRAR.0043F7F9	
0043F7F5	> 95C0	TEST EAX,EAX	
0043F7F7	> 7D 24	JGE SHORT WinRAR.0043F81D	
0043F7F9	> C605 95684A00 01	MOV BYTE PTR DS:[4A6895],1	
0043F800	> 6A 00	PUSH 0	
0043F802	> 68 302E4800	PUSH WinRAR.00482E30	
0043F807	> FF35 4C4D4C00	PUSH DWORD PTR DS:[4C4D4C]	
0043F80D	> 68 74694A00	PUSH WinRAR.004A6974	
0043F812	> FF35 48204B00	PUSH DWORD PTR DS:[4B204B]	
0043F818	> E8 17C06000	CALL <JMP,USER32,DialogBoxParamA>	
0043F81D	> 803D 94684A00 00	CMPL BYTE PTR DS:[4A6894],0	
0043F824	> 74 1C	JE SHORT WinRAR.0043F842	
0043F826	> 803D F4764C00 00	CMPL BYTE PTR DS:[4C76F4],0	
0043F82D	> 75 13	JNZ SHORT WinRAR.0043F842	
0043F82F	> C605 94684A00 00	MOV BYTE PTR DS:[4A6894],0	
0043F836	> 6A 00	PUSH 0	
0043F838	> 6A 00	PUSH 0	

Case 113 (WM_TIMER) of switch 0043F8A4

Skips dialog box

ASCII "rarkey"

```

iParam = NULL
DlgProc = WinRAR.00482E30
hOwner = 002F04C8 ('WinRAR - WinRAR (evaluation o...
pTemplate = "REMINDER"
hInst = 00400000
DialogBoxParamA

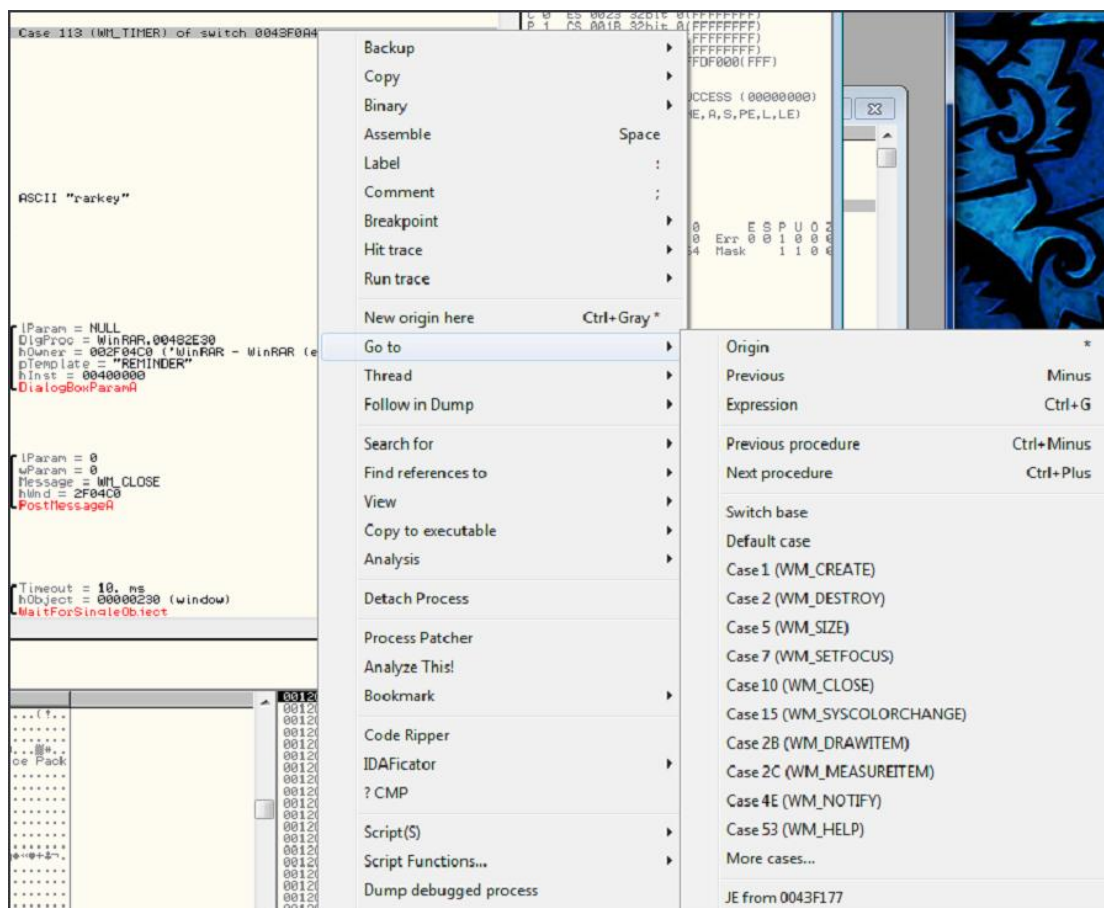
```

```

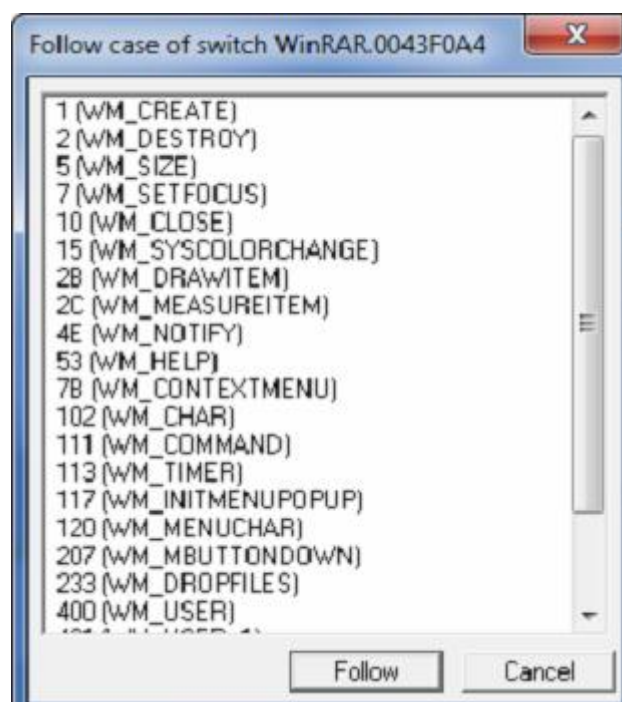
iParam = 0
iParam = 0

```

همانطور که مطلع هستید دستورالعمل پرشی در آدرس 0043F79E در صورت انجام باعث میشود nag screen نمایش داده نشود،مال بروی آدرس 0043f797 راست کلیک کنید و سپس : Go to



در قسمت Switch Case دیباگر لیست سوئیچ های مورد استفاده تایمر را لیست کرده اگر میخواهید لیست کامل را ببیند بروی More case... کلیک کنید:

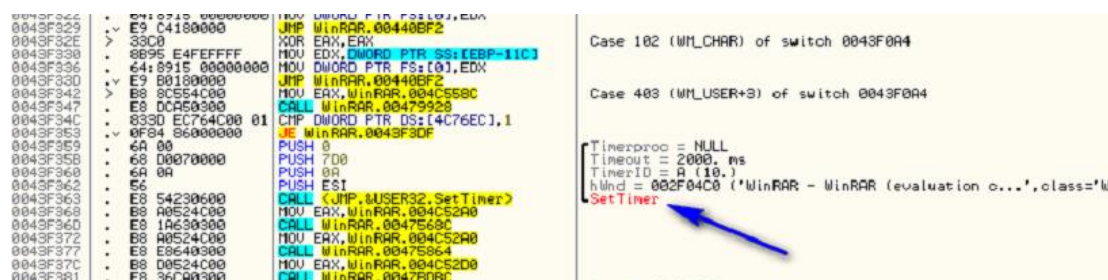


```

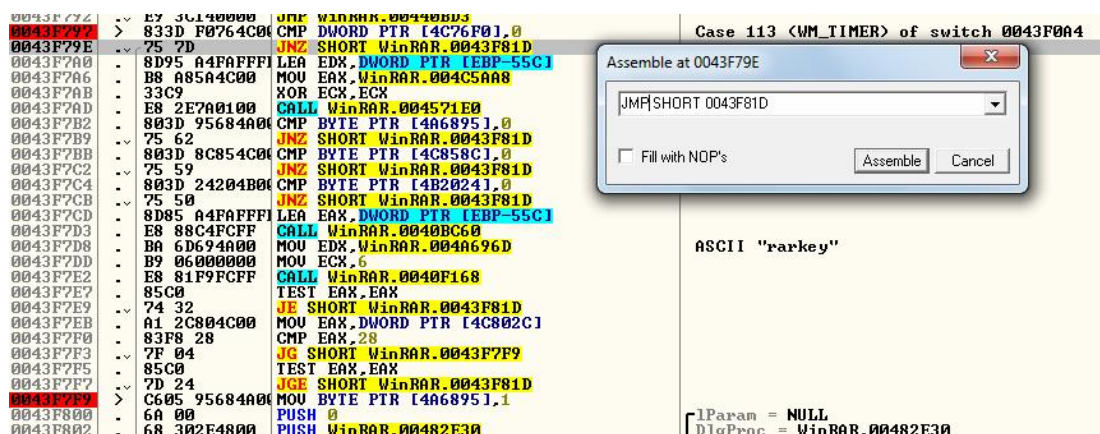
if (msg != WM_CREATE)
    jump to next if
Do WM_CREATE code
Jump to end
if (msg != WM_DESTROY)
    jump to next if
Do WM_DESTROY code
Jump to end
if (msg != WM_SIZE)
    jump to next if
Do WM_SIZE code

```

کنید آن را فواید یافت در آدرس: 43f363

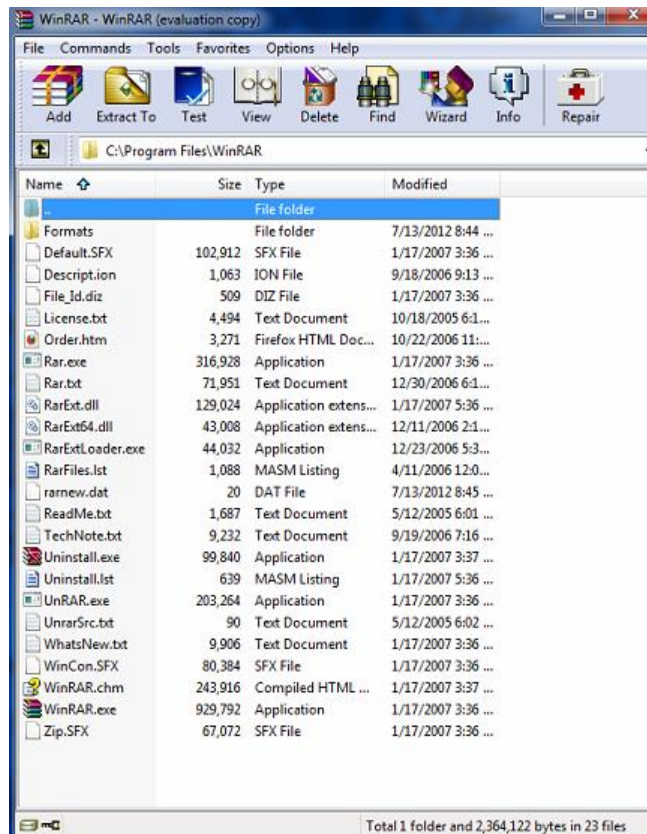


ساده ترین روش برای پی این برنامه این است که مطمئن شویم هر بار تایمر به محل نمایش دیاگ بکس می‌رسد پرش صورت می‌گیرد برای انجام اینکار به ابتدای سوئیچ (113 WM_TIMER – case) بروید و دستورالعمل JNZ را به JMP تغییر دهید :



0043F792	E9 3C140000	JMP WinRAR.00440BD3	
0043F793	833D F0764C00	CMP DWORD PTR [4C76F0],0	Case 113 <WM_TIMER> of switch 0043F0A4
0043F79E	EB 7D	JMP SHORT WinRAR.0043F81D	
0043F7A0	8D95 A4FAFFFI	LEA EDI, DWORD PTR [EBP-55C1]	
0043F7A6	B8 A85A4C00	MOV EAX, WinRAR.004C5AAB	
0043F7AB	33C9	XOR ECX, ECX	
0043F7AD	E8 2E7A0100	CALL WinRAR.004571E0	
0043F7B2	803D 95684A00	CMP BYTE PTR [4A6895],0	
0043F7B9	75 62	JNZ SHORT WinRAR.0043F81D	
0043F7BB	803D 8C854C00	CMP BYTE PTR [4C858C],0	
0043F7C2	75 59	JNZ SHORT WinRAR.0043F81D	
0043F7C4	803D 24204B00	CMP BYTE PTR [4B2024],0	
0043F7CB	75 50	JNZ SHORT WinRAR.0043F81D	
0043F7CD	8D85 A4FAFFFI	LEA EAX, DWORD PTR [EBP-55C1]	
0043F7D3	E8 88C4FCFF	CALL WinRAR.0040BC60	
0043F7D8	B8 6D694A00	MOV EDI, WinRAR.004A696D	ASCII "rarkey"
0043F7DD	B9 06000000	MOV ECX, 6	
0043F7E2	E8 81F9FCFF	CALL WinRAR.0040F168	
0043F7E7	85C0	TEST EAX, EAX	
0043F7E9	74 32	JE SHORT WinRAR.0043F81D	
0043F7EB	A1 2C804C00	MOV EAX, DWORD PTR [4C802C]	
0043F7F0	83F8 28	CMP EAX, 28	
0043F7F3	7F 04	JG SHORT WinRAR.0043F7F9	
0043F7F5	85C0	TEST EAX, EAX	
0043F7F7	7D 24	JGE SHORT WinRAR.0043F81D	
0043F7F9	C605 95684A00	MOV BYTE PTR [4A6895],1	
0043F800	6A 00	PUSH 0	lParam = NULL
0043F802	68 302E4800	PUSH WinRAR.00482E30	DlgProc = WinRAR.00482E30
0043F807	FF35 4C4D4C00	PUSH DWORD PTR [4C4D4C]	hOwner = 000B01FA <'Desktop - WinRAR (evaluation)
0043F80D	68 74694A00	PUSH WinRAR.004A6974	pTemplate = "REMINDER"
0043F812	FF35 48204B00	PUSH DWORD PTR [4B2048]	hInst = 00400000

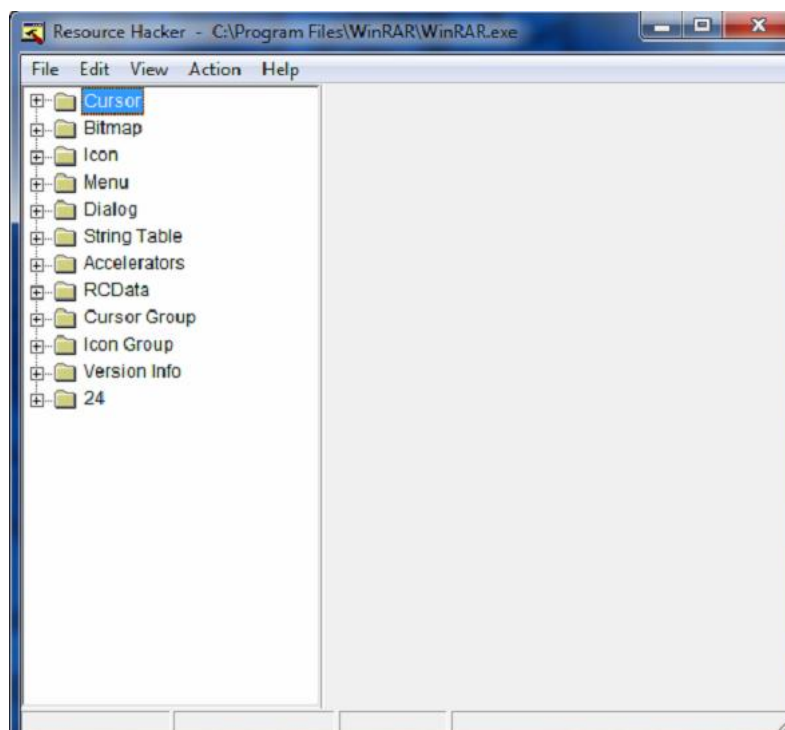
پس از مدتی متوجه میشوید که دیالوگ باکس مزاحم نمایش داده نمیشود:



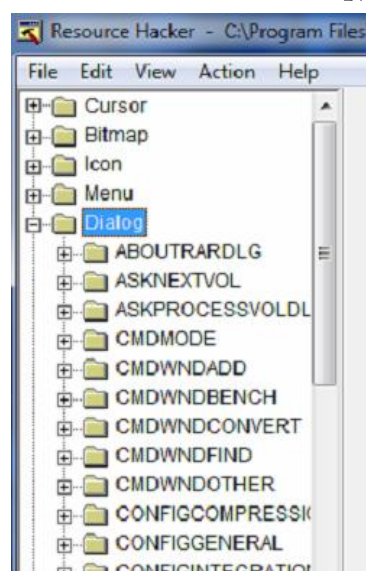
اما برنامه عبارت "evaluation" را کماکان نشان میدهد البته برنامه اکسپایر نمیشود البته اگر تغییرات در olly را ذخیره کنید ☺ به هر حال در آموزش های بعدی روش حذف این گونه پیام ها را یاد میگیریم

روش دوم:

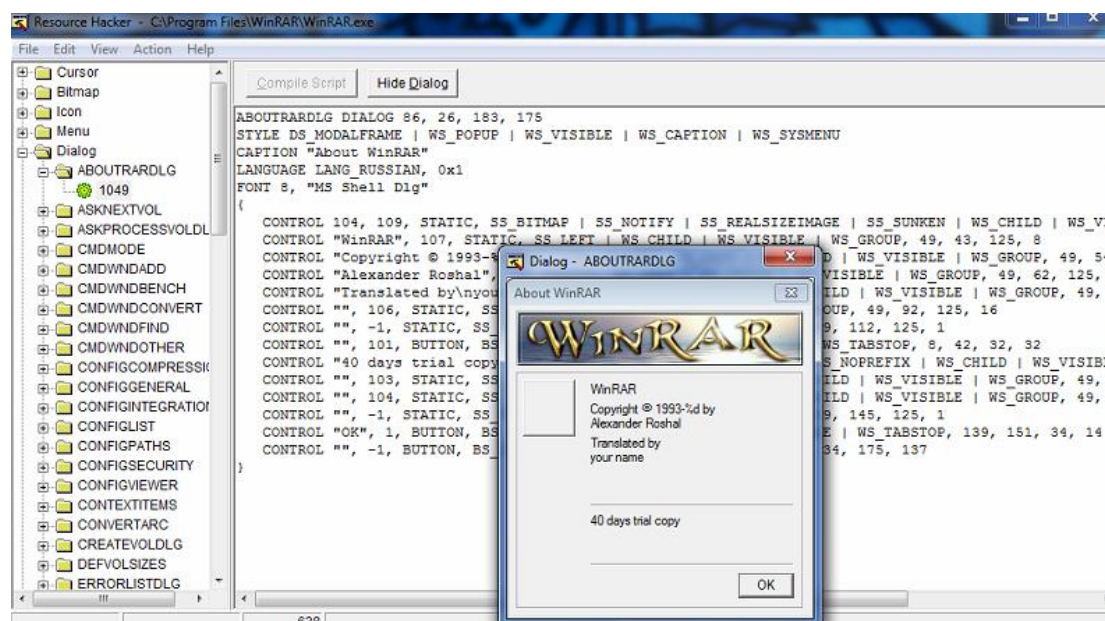
میخواهم روشی را بگویم بجای استفاده از روش اول (call stack) برای پیدا کردن دیالوگ باکس، در این روش ما از ابزاری به نام Resource Hacker استفاده میکنیم این برنامه امکان حذف، اضافه، تغییر را در منابع یک فایل PE مانند (دکمه ها، جعبه های مآوره ای، بیت مپ، آیکن ها، رشته های متن) به ما میدهد (به شرطی که این فایل اجرایی استاندارد باشد ☺)، برنامه را درون Resource Hacker باز کنید :



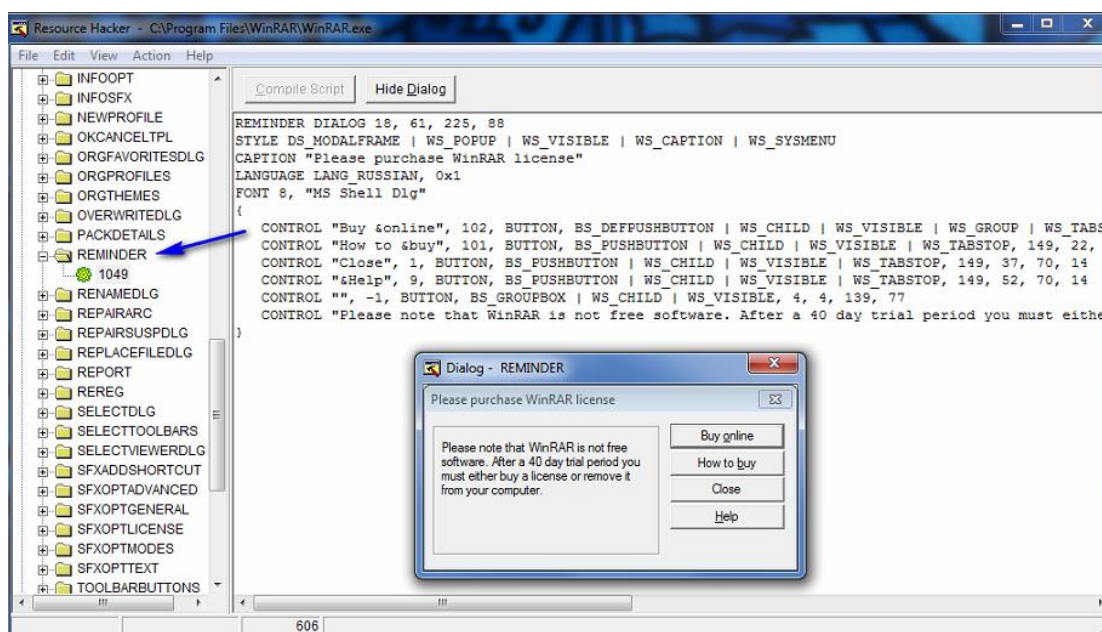
یک سافتار درفتی در سمت چپ تصویر مشاهده میکنید که شامل تمامی منابع شناخته شده ی فایل اجرایی در برنامه است، به قسمت دیالوگ بروید :



همانطور که میبیند تعداد زیادی دیالوگ باکس در برنامه وجود دارد. شما ابتدا به دنبال ABOUTRARDIALOG بگردید (اولی ☺):



Resource Hacker اطلاعات مربوط به این دیالوگ باکس ها را به ما نشان میدهد شما میتوانید آنها را تغییر دهید مال به آیتم Reminder نگاه کنید:



آشناست نه؟ بعضی موقع ها ویندوز برای ارجاعات از اسامی استفاده میکند و بعضی موقع ها از ID. در این مثال از نام استفاده کرده یعنی REMINDER حالا ما هرچیزی که نیاز داریم را میدانیم بیا به یال برگردیم و دنبال متن REMINDER بگردیم:

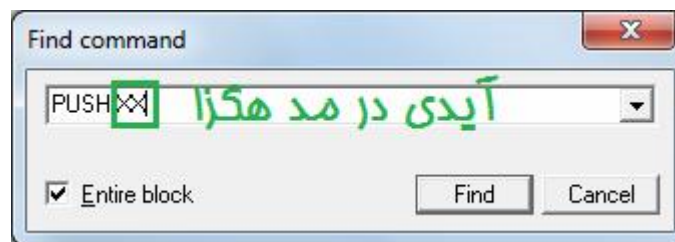
Address	Disassembly	Text string
0043F6C6	MOV EDX, WinRAR.004A691F	ASCII "HELPCommandsMenu"
0043F6EC	MOV EDX, WinRAR.004A6930	ASCII "HELPToolsMenu"
0043F712	MOV EDX, WinRAR.004A693E	ASCII "HELPFavoritesMenu"
0043F738	MOV EDX, WinRAR.004A6950	ASCII "HELPOptionsMenu"
0043F766	MOV EDX, WinRAR.004A6960	ASCII "HELPHelpMenu"
0043F79E	JMP SHORT WinRAR.0043F81D	<Initial CPU selection>
0043F7D8	MOV EDX, WinRAR.004A696D	ASCII "rarkey"
0043F80D	PUSH WinRAR.004A6974	ASCII "REMINDER"
0043FA14	PUSH WinRAR.004A697D	ASCII "%c:\\"
0043FD07	MOV EAX, WinRAR.004C5504	ASCII "ArcHistory"
0043FD2B	MOV EAX, WinRAR.004C5548	ASCII "Favorites"
004404D3	MOV EAX, WinRAR.004C5548	ASCII "Favorites"
004404F1	MOV EAX, WinRAR.004C5548	ASCII "Favorites"
004405AF	PUSH WinRAR.004C770C	ASCII "C:\Users\mo dongle\AppData\Roaming\WinRAR\rar.log"
004405F5	PUSH WinRAR.004A6982	ASCII "http://www.rarlab.com"
00440686	PUSH WinRAR.004A6998	ASCII "ABOUTRARDLG"
004406AA	MOV EDX, WinRAR.004A69A4	ASCII "-"
00440716	MOV EDX, WinRAR.004A69B0	ASCII "Detailed"

بروی متن مورد نظر دبل کلیک کنید:

Address	Disassembly	Text string
0043F7D3	CALL WinRAR.0040BC60	
0043F7D8	MOV EDX, WinRAR.004A696D	ASCII "rarkey"
0043F7DD	MOV ECX, 5	
0043F7E2	CALL WinRAR.0040F168	
0043F7E7	TEST EAX, EAX	
0043F7E9	JE SHORT WinRAR.0043F81D	
0043F7EB	MOV EAX, DWORD PTR [4C802C]	
0043F7F0	CMP EAX, 28	
0043F7F3	JG SHORT WinRAR.0043F7F9	
0043F7F5	TEST EAX, EAX	
0043F7F7	JGE SHORT WinRAR.0043F81D	
0043F7F9	CMP EAX, 24	
0043F800	MOV BYTE PTR [4A6895], 1	
0043F800	PUSH 0	
0043F802	PUSH WinRAR.00482E30	
0043F807	FF35 4C4D4C00 PUSH DWORD PTR [4C4D4C]	
0043F80D	68 74694A00 PUSH WinRAR.004A6974	
0043F812	FF35 4B204B00 PUSH DWORD PTR [4B204B]	
0043F818	EB 171C0600 CALL <JMP.&USER32.DialogBoxParamA>	
0043F81D	803D 94684A00 CMP BYTE PTR [4A6894], 0	
0043F824	74 1C JE SHORT WinRAR.0043F842	
0043F826	803D F4764C00 CMP BYTE PTR [4C76F4], 0	
0043F82D	75 13 JNZ SHORT WinRAR.0043F842	
0043F82F	C605 94684A00 MOV BYTE PTR [4A6894], 0	
0043F836	6A 00 PUSH 0	
0043F838	6A 00 PUSH 0	
0043F83A	6A 10 PUSH 10	
0043F83C	56 PUSH ESI	
0043F83D	E8 D81D0600 CALL <JMP.&USER32.PostMessageA>	
0043F842	833D F0764C00 CMP DWORD PTR [4C76F0], 0	
0043F849	75 2D JNZ SHORT WinRAR.0043F878	
0043F84B	833D E8764C00 CMP DWORD PTR [4C76E8], 0	
0043F852	75 24 JNZ SHORT WinRAR.0043F878	
0043F854	833D 08774C00 CMP DWORD PTR [4C7708], -1	
0043F85B	74 1B JE SHORT WinRAR.0043F878	
0043F85D	6A 00 PUSH 0	
0043F85F	FF35 08774C00 PUSH DWORD PTR [4C7708]	
0043F865	E8 80190600 CALL <JMP.&KERNEL32.WaitForSingleObject>	
0043F86A	85C0 TEST EAX, EAX	
0043F86C	75 0A JNZ SHORT WinRAR.0043F878	
0043F86E	B8 604D4C00 MOV EAX, WinRAR.004C4D60	

همان جایی که با تکنیک call stack داده شدیم، همانطور که در تصویر بالا میبیند آگومانهای تابع DialogBoxParamA را میبینید، مال اگر منابع با ID مشخص شده بود چه؟ در این صورت باید در پنجره ی disassembly راست کلیک کنید:

4C00 PUSH DWORD PTR [4C4D4C] 1000 PUSH WinRAR.004A6974 34B00 PUSH DWORD PTR [4B2048] 3000 CALL <JMP.&USER32.DialogBoxParamA> 34A00 CMP BYTE PTR [4A6894], 0 34C00 JE SHORT WinRAR.0043F842 34C00 CMP BYTE PTR [4C76F4], 0 34A00 JNZ SHORT WinRAR.0043F842 34A00 MOV BYTE PTR [4A6894], 0 PUSH 0 PUSH 0 PUSH 10 PUSH ESI 3000 CALL <JMP.&USER32.PostMessageA> 34C00 CMP DWORD PTR [4C76F0], 0 34C00 JNZ SHORT WinRAR.0043F878 34C00 CMP DWORD PTR [4C76E8], 0 34C00 JNZ SHORT WinRAR.0043F878 74C00 CMP DWORD PTR [4C7708], -1 JE SHORT WinRAR.0043F878 PUSH 0 74C00 PUSH DWORD PTR [4C7708] 3000 CALL <JMP.&KERNEL32.WaitForSingleObject> TEST EAX, EAX 3000 JNZ SHORT WinRAR.0043F878 MOV EAX, WinRAR.004C4D60 1000 CALL WinRAR.004591D8 774 <ASCII "REMINDER">	Backup Copy Binary Assemble Space Label Comment Breakpoint Hit trace Run trace New origin here Ctrl+ Gray * Go to Thread Follow in Dump Search for Find references to View Copy to executable Analysis	ktop - WinRAR (evaluation ...) 1 S E 2 E 3 D 4 E 5 E 6 T 7 S 8 T 9 S 10 T 11 S 12 T 13 S 14 T 15 S 16 T 17 S 18 T 19 S 20 T 21 S 22 T 23 S 24 T 25 S 26 T 27 S 28 T 29 S 30 T 31 S 32 T 33 S 34 T 35 S 36 T 37 S 38 T 39 S 40 T 41 S 42 T 43 S 44 T 45 S 46 T 47 S 48 T 49 S 50 T 51 S 52 T 53 S 54 T 55 S 56 T 57 S 58 T 59 S 60 T 61 S 62 T 63 S 64 T 65 S 66 T 67 S 68 T 69 S 70 T 71 S 72 T 73 S 74 T 75 S 76 T 77 S 78 T 79 S 80 T 81 S 82 T 83 S 84 T 85 S 86 T 87 S 88 T 89 S 90 T 91 S 92 T 93 S 94 T 95 S 96 T 97 S 98 T 99 S 100 T 101 S 102 T 103 S 104 T 105 S 106 T 107 S 108 T 109 S 110 T 111 S 112 T 113 S 114 T 115 S 116 T 117 S 118 T 119 S 120 T 121 S 122 T 123 S 124 T 125 S 126 T 127 S 128 T 129 S 130 T 131 S 132 T 133 S 134 T 135 S 136 T 137 S 138 T 139 S 140 T 141 S 142 T 143 S 144 T 145 S 146 T 147 S 148 T 149 S 150 T 151 S 152 T 153 S 154 T 155 S 156 T 157 S 158 T 159 S 160 T 161 S 162 T 163 S 164 T 165 S 166 T 167 S 168 T 169 S 170 T 171 S 172 T 173 S 174 T 175 S 176 T 177 S 178 T 179 S 180 T 181 S 182 T 183 S 184 T 185 S 186 T 187 S 188 T 189 S 190 T 191 S 192 T 193 S 194 T 195 S 196 T 197 S 198 T 199 S 200 T 201 S 202 T 203 S 204 T 205 S 206 T 207 S 208 T 209 S 210 T 211 S 212 T 213 S 214 T 215 S 216 T 217 S 218 T 219 S 220 T 221 S 222 T 223 S 224 T 225 S 226 T 227 S 228 T 229 S 230 T 231 S 232 T 233 S 234 T 235 S 236 T 237 S 238 T 239 S 240 T 241 S 242 T 243 S 244 T 245 S 246 T 247 S 248 T 249 S 250 T 251 S 252 T 253 S 254 T 255 S 256 T 257 S 258 T 259 S 260 T 261 S 262 T 263 S 264 T 265 S 266 T 267 S 268 T 269 S 270 T 271 S 272 T 273 S 274 T 275 S 276 T 277 S 278 T 279 S 280 T 281 S 282 T 283 S 284 T 285 S 286 T 287 S 288 T 289 S 290 T 291 S 292 T 293 S 294 T 295 S 296 T 297 S 298 T 299 S 300 T 301 S 302 T 303 S 304 T 305 S 306 T 307 S 308 T 309 S 310 T 311 S 312 T 313 S 314 T 315 S 316 T 317 S 318 T 319 S 320 T 321 S 322 T 323 S 324 T 325 S 326 T 327 S 328 T 329 S 330 T 331 S 332 T 333 S 334 T 335 S 336 T 337 S 338 T 339 S 340 T 341 S 342 T 343 S 344 T 345 S 346 T 347 S 348 T 349 S 350 T 351 S 352 T 353 S 354 T 355 S 356 T 357 S 358 T 359 S 360 T 361 S 362 T 363 S 364 T 365 S 366 T 367 S 368 T 369 S 370 T 371 S 372 T 373 S 374 T 375 S 376 T 377 S 378 T 379 S 380 T 381 S 382 T 383 S 384 T 385 S 386 T 387 S 388 T 389 S 390 T 391 S 392 T 393 S 394 T 395 S 396 T 397 S 398 T 399 S 400 T 401 S 402 T 403 S 404 T 405 S 406 T 407 S 408 T 409 S 410 T 411 S 412 T 413 S 414 T 415 S 416 T 417 S 418 T 419 S 420 T 421 S 422 T 423 S 424 T 425 S 426 T 427 S 428 T 429 S 430 T 431 S 432 T 433 S 434 T 435 S 436 T 437 S 438 T 439 S 440 T 441 S 442 T 443 S 444 T 445 S 446 T 447 S 448 T 449 S 450 T 451 S 452 T 453 S 454 T 455 S 456 T 457 S 458 T 459 S 460 T 461 S 462 T 463 S 464 T 465 S 466 T 467 S 468 T 469 S 470 T 471 S 472 T 473 S 474 T 475 S 476 T 477 S 478 T 479 S 480 T 481 S 482 T 483 S 484 T 485 S 486 T 487 S 488 T 489 S 490 T 491 S 492 T 493 S 494 T 495 S 496 T 497 S 498 T 499 S 500 T 501 S 502 T 503 S 504 T 505 S 506 T 507 S 508 T 509 S 510 T 511 S 512 T 513 S 514 T 515 S 516 T 517 S 518 T 519 S 520 T 521 S 522 T 523 S 524 T 525 S 526 T 527 S 528 T 529 S 530 T 531 S 532 T 533 S 534 T 535 S 536 T 537 S 538 T 539 S 540 T 541 S 542 T 543 S 544 T 545 S 546 T 547 S 548 T 549 S 550 T 551 S 552 T 553 S 554 T 555 S 556 T 557 S 558 T 559 S 560 T 561 S 562 T 563 S 564 T 565 S 566 T 567 S 568 T 569 S 570 T 571 S 572 T 573 S 574 T 575 S 576 T 577 S 578 T 579 S 580 T 581 S 582 T 583 S 584 T 585 S 586 T 587 S 588 T 589 S 590 T 591 S 592 T 593 S 594 T 595 S 596 T 597 S 598 T 599 S 600 T 601 S 602 T 603 S 604 T 605 S 606 T 607 S 608 T 609 S 610 T 611 S 612 T 613 S 614 T 615 S 616 T 617 S 618 T 619 S 620 T 621 S 622 T 623 S 624 T 625 S 626 T 627 S 628 T 629 S 630 T 631 S 632 T 633 S 634 T 635 S 636 T 637 S 638 T 639 S 640 T 641 S 642 T 643 S 644 T 645 S 646 T 647 S 648 T 649 S 650 T 651 S 652 T 653 S 654 T 655 S 656 T 657 S 658 T 659 S 660 T 661 S 662 T 663 S 664 T 665 S 666 T 667 S 668 T 669 S 670 T 671 S 672 T 673 S 674 T 675 S 676 T 677 S 678 T 679 S 680 T 681 S 682 T 683 S 684 T 685 S 686 T 687 S 688 T 689 S 690 T 691 S 692 T 693 S 694 T 695 S 696 T 697 S 698 T 699 S 700 T 701 S 702 T 703 S 704 T 705 S 706 T 707 S 708 T 709 S 710 T 711 S 712 T 713 S 714 T 715 S 716 T 717 S 718 T 719 S 720 T 721 S 722 T 723 S 724 T 725 S 726 T 727 S 728 T 729 S 730 T 731 S 732 T 733 S 734 T 735 S 736 T 737 S 738 T 739 S 740 T 741 S 742 T 743 S 744 T 745 S 746 T 747 S 748 T 749 S 750 T 751 S 752 T 753 S 754 T 755 S 756 T 757 S 758 T 759 S 760 T 761 S 762 T 763 S 764 T 765 S 766 T 767 S 768 T 769 S 770 T 771 S 772 T 773 S 774 T 775 S 776 T 777 S 778 T 779 S 780 T 781 S 782 T 783 S 784 T 785 S 786 T 787 S 788 T 789 S 790 T 791 S 792 T 793 S 794 T 795 S 796 T 797 S 798 T 799 S 800 T 801 S 802 T 803 S 804 T 805 S 806 T 807 S 808 T 809 S 810 T 811 S 812 T 813 S 814 T 815 S 816 T 817 S 818 T 819 S 820 T 821 S 822 T 823 S 824 T 825 S 826 T 827 S 828 T 829 S 830 T 831 S 832 T 833 S 834 T 835 S 836 T 837 S 838 T 839 S 840 T 841 S 842 T 843 S 844 T 845 S 846 T 847 S 848 T 849 S 850 T 851 S 852 T 853 S 854 T 855 S 856 T 857 S 858 T 859 S 860 T 861 S 862 T 863 S 864 T 865 S 866 T 867 S 868 T 869 S 870 T 871 S 872 T 873 S 874 T 875 S 876 T 8
--	--	--



یک نکته دیگر

اگر شما آموزش های دیگر کرکینگ باینری را نگاه کنید متما یکی از آنها درباره ی Resource Hacker است، با استفاده از این برنامه به راحتی میتوانید تغییراتی در برنامه بدهید البته به شرط آنکه برنامه در شرایط استاندارد باشد برای مثال پروتکت نشده باشد، همینطور در همین مثال یعنی winrar میتوانید برای حذف nag screen از آن بهره ببرید.

تا آموزش بعدی...

یادتون نره ساعت سیستمتون رو برگردونید ☺