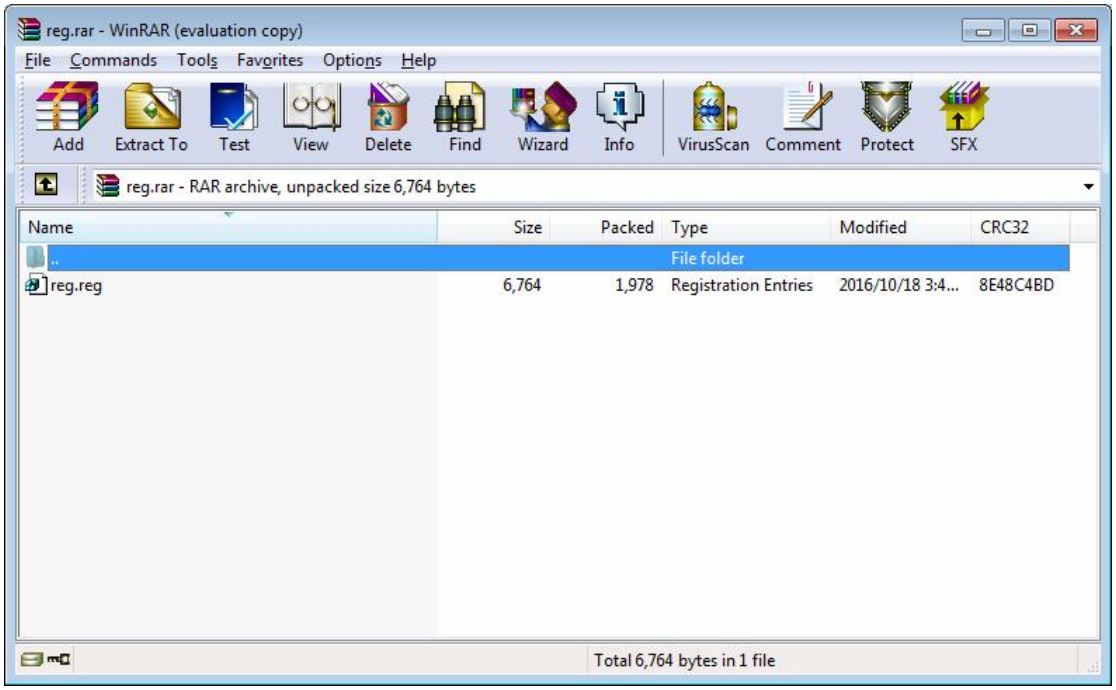
سری آموزش های R4NDOM-فارسی

قسمت 15- استفاده از Call Stack

در این قسمت ما محدودیت Nag Screen یک برنامه واقعی (WinRAR ضمیمه 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 همینطور با کم ترین آسیب به ساختار 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 میخواهم 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 میدهیم متوجه میشویم که بعد از 40 روز (نویسنده:درست اندازه ی زمان روزه داری حضرت 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.



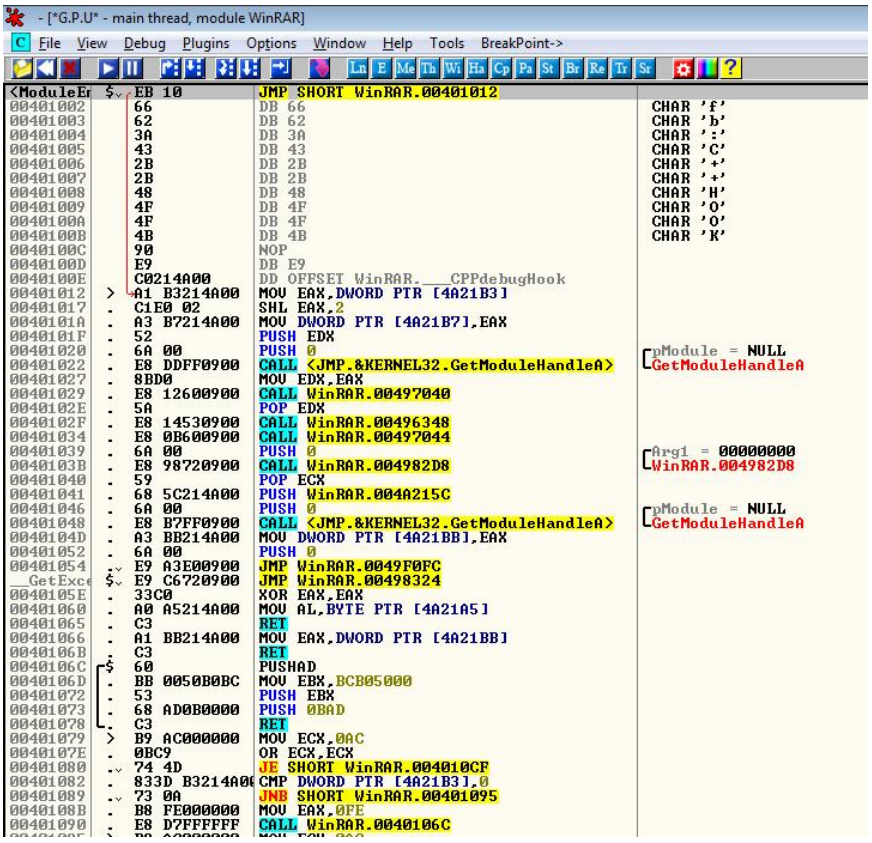
و بعد از 40 روز :

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 تحت دیباگر اجرا کنید تا Nag Screen ظاهر شود، قبل از آنکه آن را ببندید بروی Pause کلیک کنید تا Olly موقتا متوقف شود:

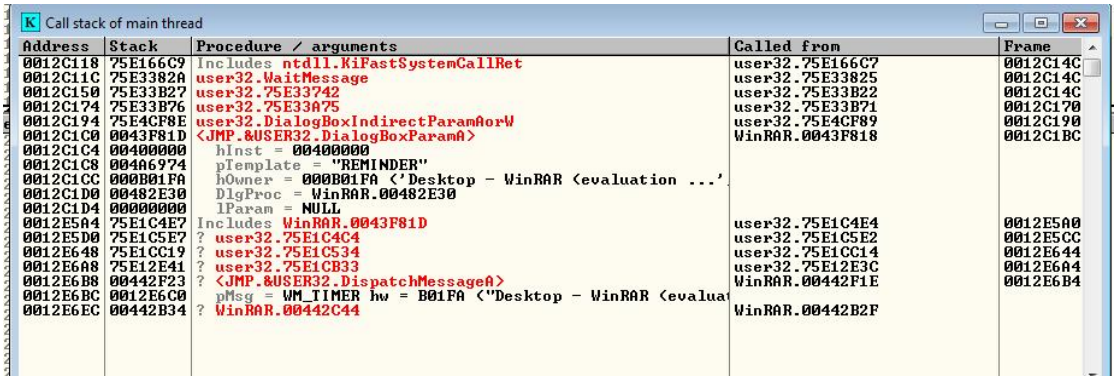
حالا ما میخواهیم بدانیم که این Nag از کجا آمده است.البته میتوان از تکنیک های intermodular callsو جستجوی رشته ها بهره برد اما به شما قول میدهم که به اندازه ی این تکنیک نمیتواند مفید باشد.همینطور از این تکنیک میتوان برای بسیاری از برنامه ها به کاربرد حتی زمانی که رشته ایی وجود ندارد استفاده کرد ،گذشته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

Call Stack

اکثر کامپایلرها برای فراخوانی و برگشت زیربرنامه **فراخوانی پشته** (call stack) را پیاده‌سازی می‌کنند . Call stackیا run-time stack یک پشته است که اطلاعاتی درباره زیربرنامه فعال یک برنامه را نگهداری می‌کند. زیربرنامه فعال زیربرنامه‌ای است که فراخوانی شده‌است اما هنوز اجرایش تمام نشده‌است.

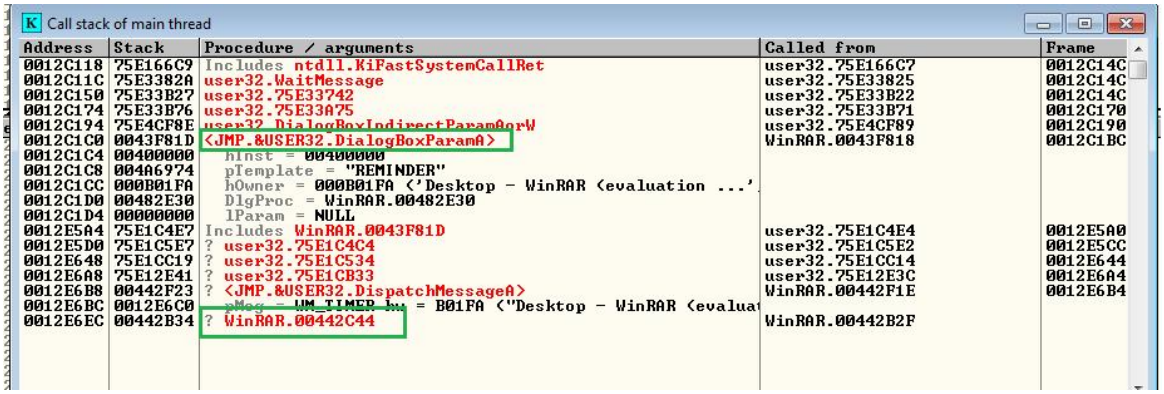
OllyDBG هم با ردیابی فراخوانی فعال محل آن را نمایش میدهد همچنین سعی میکند که آرگومان های انتقال داده شده ی مربوط به تابع را نمایش دهد تمامی این فرایند ها روند طبیعی Stack است و آن را میتوان در پنجره ی Stack (پایین سمت راست OllyDBG) دید، اما یادتان باشد ollydbg در این زمینه کامل نیست ، (Call Stack) و بلطبع 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 خالی هست(برنامه های vb توابع را مانند زبان های برنامه نویسی واقعیی فراخوانی نمیکنند) ،برای نمایش پنجره ی Call Stack کلید "St" مخفف Stack در نسخه ی R4NDOM یا اگراز نسخه ی اورجینال استفاده میکنید دکمه ی 'K' را بفشارید در زبان مادری نویسنده دیباگر احتمالا با K شروع میشود :

بعد از فشردن :



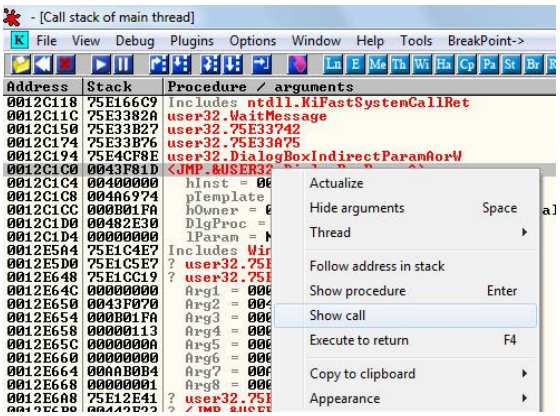
چند نکته در تصویر بالا قابل ذکر است ،اول اینکه در ابتدای اولین Call که در بالا میبینیم عبارت 'Includes' درج شده که به معنی درگیر بودن دستورالعمل به وسیله ی این Call است، ولی Olly دقیقا نمیتواند چگونگی آن را مشخص کند،در این مثال ما در ابتدا تابع ntdll را میبینیم ،همینطور در پاینتر تعدادی تابع user32 را میبینیم.که تابع DialogBoxParamA و DialogBoxIndirectParamAorW با آرگومان های خود فراخوانی شده اند، و همینطور در پاینتر تعدادی Call دیگرمربوط به user32 داریم و در خط آخر winrarدر آدرس 00442C44 تابع DispatchMessageA فراخوانی شده

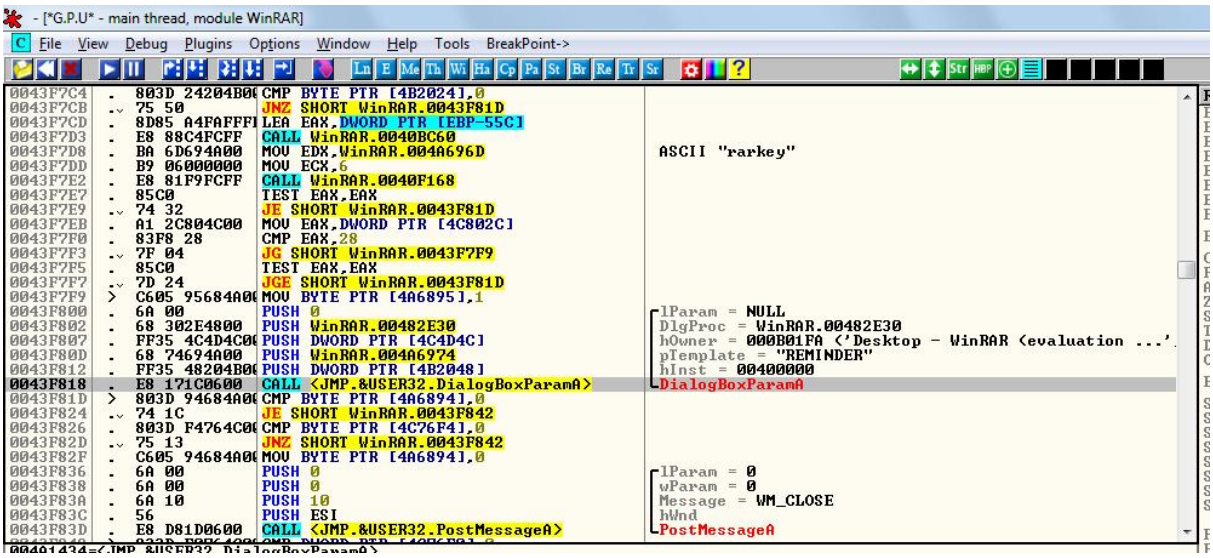
همچنین تابع DialogBoxParamA در User32 مسئول نمایش دیالوگ باکس و متن "evaluation copy" است و پس از نمایش دیالوگ باکس و متن مورد نظر منتظر ورودی کاربر با استفاده از تابع WaitMessage میشود:



مهمترین چیز در این پنجره فراخوانی دیالوگ باکس و محل آن در برنامه ما است،معمولا وقتی از call stackاستفاده میکنیم، از بالای پنجره ی Stackشروع 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 دیالوگ باکس میگذارم :

اگر به بالا نگاه کنید چند پرش شرطی میبینید و همینطور اگر کمی به بالا (کمی به بالا اسکرول کنید و به قسمت کامنت دستورات نگاه کنید) (که به معنای تلاش مقایسه میباشد “Case XXX”)

(WM_Something) را خواهید 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 ECX,ECX
0043F76D  .  8BC6          MOV EAX,ESI
0043F76F  .  E8 A8470200   CALL WinRAR.00463F1C
0043F774  .v 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  .v 0F85 4B140000 JNZ WinRAR.00440BD3
0043F788  .  B8 604D4C00   MOV EAX,WinRAR.004C4D60
0043F78D  .  E8 4ACD0100   CALL WinRAR.0045C4DC
0043F792  .v E9 3C140000   JMP WinRAR.00440BD3
0043F797  >  833D F0764C00 CMP DWORD PTR [4C76F0],0         Case 113 (WM_TIMER) of switch 0043F0A4
0043F79E  .v 75 7D         JNZ SHORT WinRAR.0043F81D
0043F7A0  .  8D95 A4FAFFFI LEA EDX,DWORD PTR [EBP-55C]
0043F7A6  .  B8 A85A4C00   MOV EAX,WinRAR.004C5AA8
0043F7AB  .  33C9          XOR ECX,ECX
0043F7AD  .  E8 2E7A0100   CALL WinRAR.004571E0
0043F7B2  .  803D 95684A00 CMP BYTE PTR [4A6895],0
0043F7B9  .v 75 62         JNZ SHORT WinRAR.0043F81D
0043F7BB  .  803D 8C854C00 CMP BYTE PTR [4C858C],0
0043F7C2  .v 75 59         JNZ SHORT WinRAR.0043F81D
0043F7C4  .  803D 24204B00 CMP BYTE PTR [4B2024],0
0043F7CB  .v 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          ASCII "rarkey"
0043F7DD  .  B9 06000000   MOV ECX,6
0043F7E2  .  E8 81F9FCFF   CALL WinRAR.0040F168
0043F7E7  .  85C0          TEST EAX,EAX
0043F7E9  .v 74 32         JE SHORT WinRAR.0043F81D
0043F7EB  .  A1 2C804C00   MOV EAX,DWORD PTR [4C802C]
0043F7F0  .  83F8 28       CMP EAX,28
0043F7F3  .v 7F 04         JG SHORT WinRAR.0043F7F9
0043F7F5  .  85C0          TEST EAX,EAX
0043F7F7  .v 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
```

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

```
File View Debug Plugins Options Window Help Tools BreakPoint->
0043F766  .  BA 60694A00   MOV EDX,WinRAR.004A6960          ASCII "HELPHelpMenu"
0043F76B  .  33C9          XOR ECX,ECX
0043F76D  .  8BC6          MOV EAX,ESI
0043F76F  .  E8 A8470200   CALL WinRAR.00463F1C
0043F774  .v 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  .v 0F85 4B140000 JNZ WinRAR.00440BD3
0043F788  .  B8 604D4C00   MOV EAX,WinRAR.004C4D60
0043F78D  .  E8 4ACD0100   CALL WinRAR.0045C4DC
0043F792  .v E9 3C140000   JMP WinRAR.00440BD3
0043F797  >  833D F0764C00 CMP DWORD PTR [4C76F0],0         Case 113 (WM_TIMER) of switch 0043F0A4
0043F79E  .v 75 7D         JNZ SHORT WinRAR.0043F81D
0043F7A0  .  8D95 A4FAFFFI LEA EDX,DWORD PTR [EBP-55C]
0043F7A6  .  B8 A85A4C00   MOV EAX,WinRAR.004C5AA8
0043F7AB  .  33C9          XOR ECX,ECX
0043F7AD  .  E8 2E7A0100   CALL WinRAR.004571E0
0043F7B2  .  803D 95684A00 CMP BYTE PTR [4A6895],0
0043F7B9  .v 75 62         JNZ SHORT WinRAR.0043F81D
0043F7BB  .  803D 8C854C00 CMP BYTE PTR [4C858C],0
0043F7C2  .v 75 59         JNZ SHORT WinRAR.0043F81D
0043F7C4  .  803D 24204B00 CMP BYTE PTR [4B2024],0
0043F7CB  .v 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          ASCII "rarkey"
0043F7DD  .  B9 06000000   MOV ECX,6
0043F7E2  .  E8 81F9FCFF   CALL WinRAR.0040F168
0043F7E7  .  85C0          TEST EAX,EAX
0043F7E9  .v 74 32         JE SHORT WinRAR.0043F81D
0043F7EB  .  A1 2C804C00   MOV EAX,DWORD PTR [4C802C]
0043F7F0  .  83F8 28       CMP EAX,28
0043F7F3  .v 7F 04         JG SHORT WinRAR.0043F7F9
0043F7F5  .  85C0          TEST EAX,EAX
0043F7F7  .v 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
DS:[004C76F0]=00000000
Jump from 0043F177
```

همان طور که میدانید قسمت WM_TIMER بازگو کننده ی خیلی 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  .v 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
0043F818  . E8 171C0600   CALL <JMP.&USER32.DialogBoxParamA>   DialogBoxParamA
0043F81D  > 803D 94684A00 CMP BYTE PTR [4A6894],0
0043F824  .v 74 1C        JE SHORT WinRAR.0043F842
0043F826  . 803D F4764C00 CMP BYTE PTR [4C76F4],0
0043F82D  .v 75 13        JNZ SHORT WinRAR.0043F842
0043F82F  . C605 94684A00 MOV BYTE PTR [4A6894],0
```

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

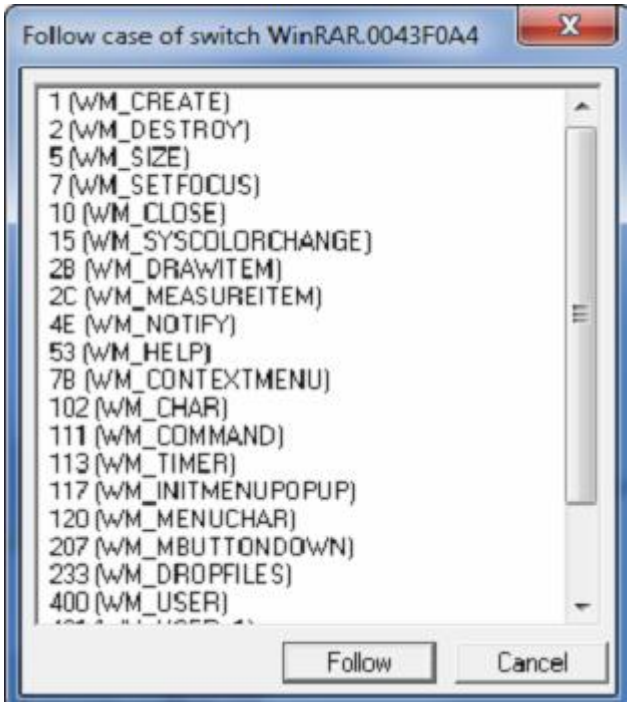
خب برمیگردیم به قسمت مورد نظر یعنی ابتدای سوئیچ تایمر در آدرس :43F797 یک BP بگذارید (اگر قبلا نگذاشته اید):

```
0043F782  .v 0F85 4B140000 JNZ WinRAR.00440BD3
0043F788  . B8 604D4C00    MOV EAX,WinRAR.004C4D60
0043F78D  . E8 4ACD0100    CALL WinRAR.0045C4DC
0043F792  .v E9 3C140000   JMP WinRAR.00440BD3
0043F797  > 833D F0764C00 00 CMP DWORD PTR DS:[4C76F0],0   Case 113 (WM_TIMER) of switch 0043F0A4
0043F79E  .v 75 7D         JNZ SHORT WinRAR.0043F81D
0043F7A0  . 8D95 A4FAFFFF  LEA EDX,DWORD PTR SS:[EBP-55C]
0043F7A6  . B9 A85A4C00    MOV EAX,WinRAR.004C5AA8
0043F7AB  . 33C9           XOR ECX,ECX
0043F7AD  . E8 2E7A0100    CALL WinRAR.004571E0
0043F7B2  . 803D 95684A00 00 CMP BYTE PTR DS:[4A6895],0
0043F7B9  .v 75 62         JNZ SHORT WinRAR.0043F81D
0043F7BB  . 803D 8C854C00 00 CMP BYTE PTR DS:[4C858C],0
0043F7C2  .v 75 59         JNZ SHORT WinRAR.0043F81D
0043F7C4  . 803D 24204B00 00 CMP BYTE PTR DS:[4B2024],0
0043F7CB  .v 75 50         JNZ SHORT WinRAR.0043F81D
0043F7CD  . 8D85 A4FAFFFF  LEA EAX,DWORD PTR SS:[EBP-55C]
0043F7D3  . E8 88C4FCFF    CALL WinRAR.0040BC60
0043F7D8  . BA 6D694A00    MOV EDX,WinRAR.004A696D        ASCII "rarkey"
0043F7DD  . B9 06000000    MOV ECX,6
0043F7E2  . E8 81F9FCFF    CALL WinRAR.0040F168
0043F7E7  . 85C0           TEST EAX,EAX
0043F7E9  .v 74 32         JE SHORT WinRAR.0043F81D
0043F7EB  . A1 2C804C00    MOV EAX,DWORD PTR DS:[4C802C]
0043F7F0  . 83F8 28        CMP EAX,28
0043F7F3  .v 7F 04         JG SHORT WinRAR.0043F7F9
0043F7F5  . 85C0           TEST EAX,EAX
0043F7F7  .v 7D 24         JGE SHORT WinRAR.0043F81D
0043F7F9  > C605 95684A00 01 MOV BYTE PTR DS:[4A6895],1
0043F800  . 6A 00          PUSH 0                          lParam = NULL
0043F802  . 68 302E4800    PUSH WinRAR.00482E30            DlgProc = WinRAR.00482E30
0043F807  . FF35 4C4D4C00  PUSH DWORD PTR DS:[4C4D4C]      hOwner = 002F04C0 ('WinRAR - WinRAR (evaluation c...
0043F80D  . 68 74694A00    PUSH WinRAR.004A6974            pTemplate = "REMINDER"
0043F812  . FF35 48204B00  PUSH DWORD PTR DS:[4B2048]      hInst = 00400000
0043F818  . E8 171C0600    CALL <JMP.&USER32.DialogBoxParamA>   DialogBoxParamA
0043F81D  > 803D 94684A00 00 CMP BYTE PTR DS:[4A6894],0
0043F824  .v 74 1C         JE SHORT WinRAR.0043F842
0043F826  . 803D F4764C00 00 CMP BYTE PTR DS:[4C76F4],0
0043F82D  .v 75 13         JNZ SHORT WinRAR.0043F842
0043F82F  . C605 94684A00 00 MOV BYTE PTR DS:[4A6894],0
0043F836  . 6A 00          PUSH 0                          lParam = 0
0043F838  . 6A 00          PUSH 0                          wParam = 0
```

Skips dialog box

همانطور که مطلع هستید دستورالعمل پرشی در آدرس 0043F79E درصورت انجام باعث میشود nag screen نمایش داده نشود،حال 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 کلید کنید:



با انتخاب هر کدام به محل آن ارجاع داده خواهید شد اگر بخواهیم ساختار سویچ را در یک شبه زبان قابل فهم توضیح بدهم اینگونه خواهد بود:

```
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
…
```

از آنجایی که مورد WM_TIMER برای ما مهم است پس تمرکز خود را بروی آن میگذاریم شما میتوانید اطلاعاتی در باره آن از گوگل به دست بیاورید که حالت آن اگر خاموش باشد چگونه است ،اما چیزی که واضح است این است که این تایمر باید از جایی شروع شده باشد اگر کمی اسکرول به بالا کنید آن را خواهید یافت در آدرس: 43f363

```
0043F329  .v E9 C4180000    JMP WinRAR.00440BF2
0043F32E  > 33C0            XOR EAX,EAX
0043F330  . 8B95 E4FEFFFF   MOV EDX,DWORD PTR SS:[EBP-11C]
0043F336  . 64:8915 00000000 MOV DWORD PTR FS:[0],EDX
0043F33D  .v E9 B0180000    JMP WinRAR.00440BF2
0043F342  > B8 8C554C00     MOV EAX,WinRAR.004C558C
0043F347  . E8 DCA50300     CALL WinRAR.00479928
0043F34C  . 833D EC764C00 01 CMP DWORD PTR DS:[4C76EC],1
0043F353  .v 0F84 86000000  JE WinRAR.0043F3DF
0043F359  . 6A 00           PUSH 0
0043F35B  . 68 D0070000     PUSH 7D0
0043F360  . 6A 0A           PUSH 0A
0043F362  . 56              PUSH ESI
0043F363  . E8 54230600     CALL <JMP.&USER32.SetTimer>
0043F368  . B8 A0524C00     MOV EAX,WinRAR.004C52A0
0043F36D  . E8 1A630300     CALL WinRAR.0047568C
0043F372  . B8 A0524C00     MOV EAX,WinRAR.004C52A0
0043F377  . E8 E8640300     CALL WinRAR.0047564
0043F37C  . B8 D0524C00     MOV EAX,WinRAR.004C52D0
0043F381  . E8 36CA0300     CALL WinRAR.0047BDBC

Case 102 (WM_CHAR) of switch 0043F0A4

Case 403 (WM_USER+3) of switch 0043F0A4

Timerproc = NULL
Timeout = 2000. ms
TimerID = A (10.)
hWnd = 002F04C0 ('WinRAR - WinRAR (evaluation o...',class='Wi
SetTimer
```

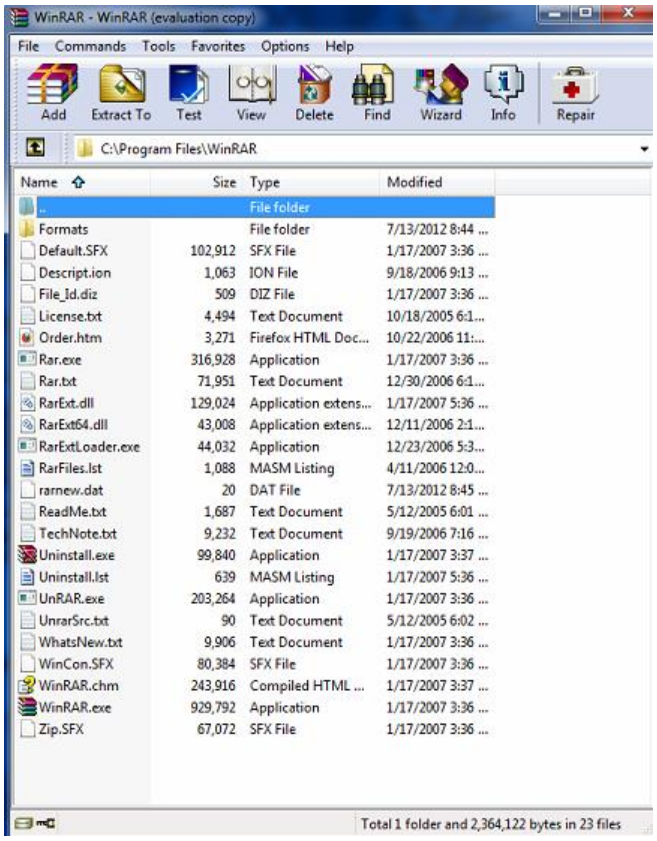
پچ کردن برنامه

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

```
0043F797  > 833D F0764C00 CMP DWORD PTR [4C76F0],0
0043F79E  .v 75 7D        JNZ SHORT WinRAR.0043F81D
0043F7A0  . 8D95 A4FAFFFF LEA EDX,DWORD PTR [EBP-55C]
0043F7A6  . B8 A85A4C00   MOV EAX,WinRAR.004C5AA8
0043F7AB  . 33C9          XOR ECX,ECX
0043F7AD  . E8 2E7A0100   CALL WinRAR.004571E0
0043F7B2  . 803D 95684A00 CMP BYTE PTR [4A6895],0
0043F7B9  .v 75 62        JNZ SHORT WinRAR.0043F81D
0043F7BB  . 803D 8C854C00 CMP BYTE PTR [4C858C],0
0043F7C2  .v 75 59        JNZ SHORT WinRAR.0043F81D
0043F7C4  . 803D 24204B00 CMP BYTE PTR [4B2024],0
0043F7CB  .v 75 50        JNZ SHORT WinRAR.0043F81D
0043F7CD  . 8D85 A4FAFFFF LEA EAX,DWORD PTR [EBP-55C]
0043F7D3  . E8 88C4FCFF   CALL WinRAR.0040BC60
0043F7D8  . BA 6D694A00   MOV EDX,WinRAR.004A696D
0043F7DD  . B9 06000000   MOV ECX,6
0043F7E2  . E8 81F9FCFF   CALL WinRAR.0040F168
0043F7E7  . 85C0          TEST EAX,EAX
0043F7E9  .v 74 32        JE SHORT WinRAR.0043F81D
0043F7EB  . A1 2C804C00   MOV EAX,DWORD PTR [4C802C]
0043F7F0  . 83F8 28       CMP EAX,28
0043F7F3  .v 7F 04        JG SHORT WinRAR.0043F7F9
0043F7F5  . 85C0          TEST EAX,EAX
0043F7F7  .v 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

Case 113 (WM_TIMER) of switch 0043F0A4

Assemble at 0043F79E
JMP SHORT 0043F81D
Fill with NOP's
Assemble
Cancel

ASCII "rarkey"

lParam = NULL
DlgProc = WinRAR.00482E30
```

```
0043F792  .v  E9 3C140000  JMP WinRAR.00440BD3
0043F797  >   833D F0764C0( CMP DWORD PTR [4C76F0],0          Case 113 (WM_TIMER) of switch 0043F0A4
0043F79E  .v  EB 7D        JMP SHORT WinRAR.0043F81D
0043F7A0  .   8D95 A4FAFFF( LEA EDX,DWORD PTR [EBP-55C]
0043F7A6  .   B8 A85A4C00  MOV EAX,WinRAR.004C5AA8
0043F7AB  .   33C9         XOR ECX,ECX
0043F7AD  .   E8 2E7A0100  CALL WinRAR.004571E0
0043F7B2  .   803D 95684A0( CMP BYTE PTR [4A6895],0
0043F7B9  .v  75 62        JNZ SHORT WinRAR.0043F81D
0043F7BB  .   803D 8C854C0( CMP BYTE PTR [4C858C],0
0043F7C2  .v  75 59        JNZ SHORT WinRAR.0043F81D
0043F7C4  .   803D 24204B0( CMP BYTE PTR [4B2024],0
0043F7CB  .v  75 50        JNZ SHORT WinRAR.0043F81D
0043F7CD  .   8D85 A4FAFFF( LEA EAX,DWORD PTR [EBP-55C]
0043F7D3  .   E8 88C4FCFF  CALL WinRAR.0040BC60
0043F7D8  .   BA 6D694A00  MOV EDX,WinRAR.004A696D           ASCII "rarkey"
0043F7DD  .   B9 06000000  MOV ECX,6
0043F7E2  .   E8 81F9FCFF  CALL WinRAR.0040F168
0043F7E7  .   85C0         TEST EAX,EAX
0043F7E9  .v  74 32        JE SHORT WinRAR.0043F81D
0043F7EB  .   A1 2C804C00  MOV EAX,DWORD PTR [4C802C]
0043F7F0  .   83F8 28      CMP EAX,28
0043F7F3  .v  7F 04        JG SHORT WinRAR.0043F7F9
0043F7F5  .   85C0         TEST EAX,EAX
0043F7F7  .v  7D 24        JGE SHORT WinRAR.0043F81D
0043F7F9  >   C605 95684A0( MOV BYTE PTR [4A6895],1
0043F800  .   6A 00        PUSH 0                            lParam = NULL
0043F802  .   68 302E4800  PUSH WinRAR.00482E30              DlgProc = WinRAR.00482E30
0043F807  .   FF35 4C4D4C0( PUSH DWORD PTR [4C4D4C]          hOwner = 000B01FA ('Desktop - WinRAR (evaluati
0043F80D  .   68 74694A00  PUSH WinRAR.004A6974              pTemplate = "REMINDER"
0043F812  .   FF35 48204B0( PUSH DWORD PTR [4B2048]          hInst = 00400000
```

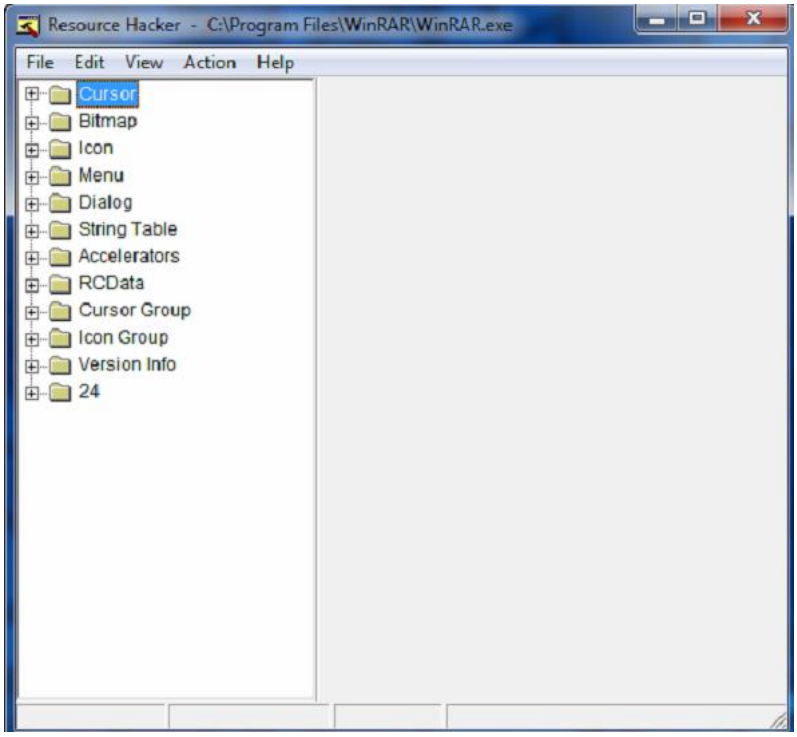
پس از مدتی متوجه میشوید که دیالوگ باکس مزاحم نمایش داده نمیشود:



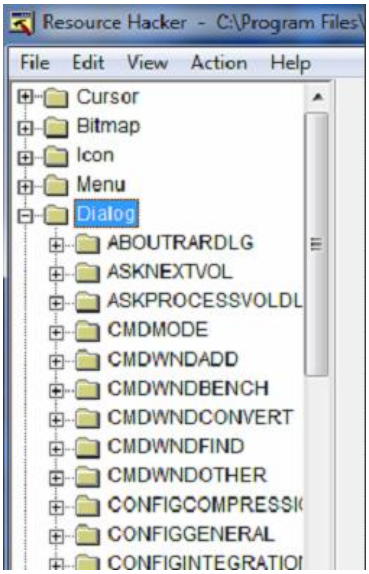
اما برنامه عبارت "evaluation" را کماکان نشان میدهد البته برنامه اکسپایر نمیشود البته اگر تغییرات در olly را ذخیره کنید ☺ به هرحال در آموزش های بعدی روش حذف این گونه پیام ها را یاد میگیریم

روش دوم:

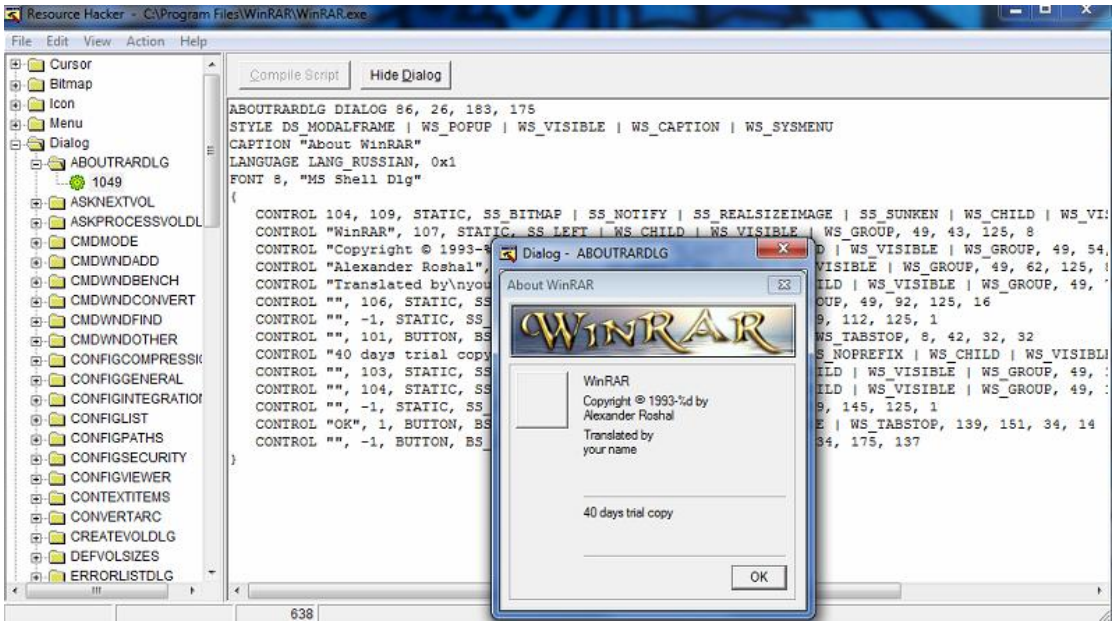
میخواهم روشی را بگویم بجای استفاده از روش اول (call stack) برای پیدا کردن دیالوگ باکس ،در این روش ما از ابزاری به نام Resource Hacker استفاده میکنیم این برنامه امکان حذف،اضافه،تغییر را در منابع یک فایل PE مانند (دکمه ها، جعبه های محاوره ای، بیت مپ، آیکون ها، رشته های متن) به ما میدهد (به شرطی که این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



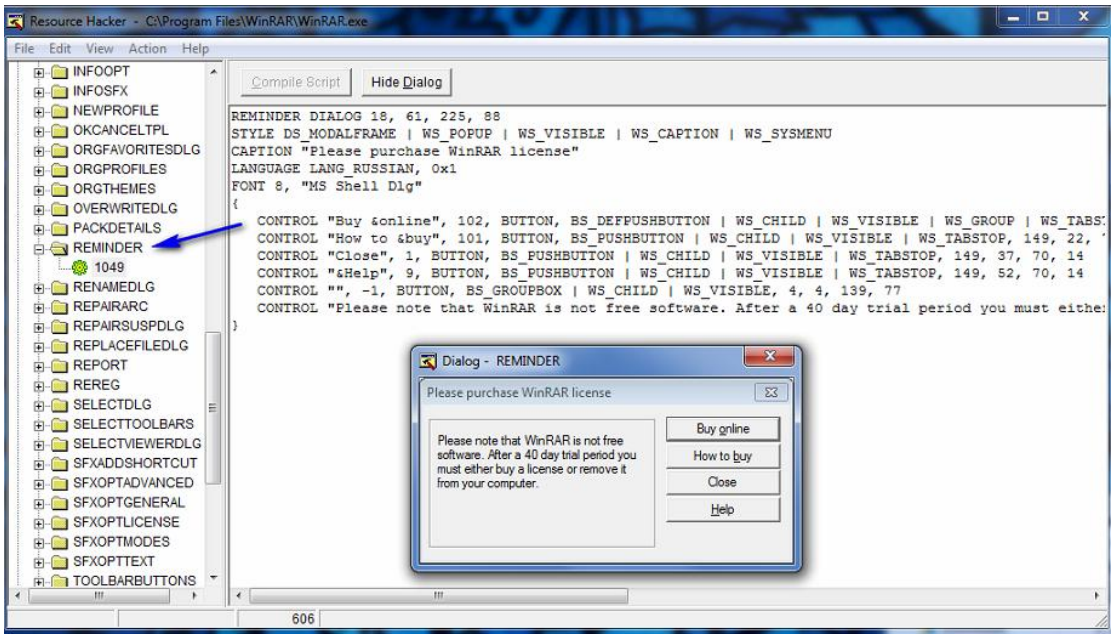
یک ساختار درختی در سمت چپ تصویر مشاهده میکنید که شامل تمامی منابع شناخته شده ی فایل اجرایی در برنامه است،به قسمت دیالوگ بروید :



همانطور که میبیند تعداد زیادی دیالوگ باکس در برنامه وجود دارد ،شماابتدا 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 حال 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 بیایید به olly برگردیم و دنبال متن REMINDER بگردیم:

```
File View Debug Plugins Options Window Help Tools BreakPoint->

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\no 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:

```
File View Debug Plugins Options Window Help Tools BreakPoint->

0043F7D3  .  E8 88C4FCFF   CALL WinRAR.0040BC60
0043F7D8  .  BA 6D694A00   MOV EDX,WinRAR.004A696D          ASCII "rarkey"
0043F7DD  .  B9 06000000   MOV ECX,6
0043F7E2  .  E8 81F9FCFF   CALL WinRAR.0040F168
0043F7E7  .  85C0          TEST EAX,EAX
0043F7E9  .v 74 32         JE SHORT WinRAR.0043F81D
0043F7EB  .  A1 2C804C00   MOV EAX,DWORD PTR [4C802C]
0043F7F0  .  83F8 28       CMP EAX,28
0043F7F3  .v 7F 04         JG SHORT WinRAR.0043F7F9
0043F7F5  .  85C0          TEST EAX,EAX
0043F7F7  .v 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
0043F818  .  E8 171C0600   CALL <JMP.&USER32.DialogBoxParamA>  DialogBoxParamA
0043F81D  >  803D 94684A00 CMP BYTE PTR [4A6894],0
0043F824  .v 74 1C         JE SHORT WinRAR.0043F842
0043F826  .  803D F4764C00 CMP BYTE PTR [4C76F4],0
0043F82D  .v 75 13         JNZ SHORT WinRAR.0043F842
0043F82F  .  C605 94684A00 MOV BYTE PTR [4A6894],0
0043F836  .  6A 00         PUSH 0                           lParam = 0
0043F838  .  6A 00         PUSH 0                           wParam = 0
0043F83A  .  6A 10         PUSH 10                          Message = WM_CLOSE
0043F83C  .  56            PUSH ESI                         hWnd
0043F83D  .  E8 D81D0600   CALL <JMP.&USER32.PostMessageA>  PostMessageA
0043F842  >  833D F0764C00 CMP DWORD PTR [4C76F0],0
0043F849  .v 75 2D         JNZ SHORT WinRAR.0043F878
0043F84B  .  833D E8764C00 CMP DWORD PTR [4C76E8],0
0043F852  .v 75 24         JNZ SHORT WinRAR.0043F878
0043F854  .  833D 08774C00 CMP DWORD PTR [4C7708],-1
0043F85B  .v 74 1B         JE SHORT WinRAR.0043F878
0043F85D  .  6A 0A         PUSH 0A                          Timeout = 10. ms
0043F85F  .  FF35 08774C00 PUSH DWORD PTR [4C7708]          hObject = 0000000C
0043F865  .  E8 8019060 0  CALL <JMP.&KERNEL32.WaitForSingleObject>  WaitForSingleObject
0043F86A  .  85C0          TEST EAX,EAX
0043F86C  .v 75 0A         JNZ SHORT WinRAR.0043F878
0043F86E  .  B8 604D4C00   MOV EAX,WinRAR.004C4D60
```

☺همان جایی که با تکنیک call stack ارجاع داده شدیم،همانطور که در تصویر بالا میبیند آرگومانهای تابع DialogBoxParamA را میبینید،حال اگر منابع با ID مشخص شده بود چه؟در این صورت باید در پنجره ی disassemblyراست کلیک کنید:

```
PUSH DWORD PTR [4C4D4C]
PUSH WinRAR.004A6974
PUSH DWORD PTR [4B2048]
CALL <JMP.&USER32.DialogBoxPa
CMP BYTE PTR [4A6894],0
JE SHORT WinRAR.0043F842
CMP BYTE PTR [4C76F4],0
JNZ SHORT WinRAR.0043F842
MOV BYTE PTR [4A6894],0
PUSH 0
PUSH 0
PUSH 10
PUSH ESI
CALL <JMP.&USER32.PostMessage
CMP DWORD PTR [4C76F0],0
JNZ SHORT WinRAR.0043F878
CMP DWORD PTR [4C76E8],0
JNZ SHORT WinRAR.0043F878
CMP DWORD PTR [4C7708],-1
JE SHORT WinRAR.0043F878
PUSH 0A
PUSH DWORD PTR [4C7708]
CALL <JMP.&KERNEL32.WaitForSi
TEST EAX,EAX
JNZ SHORT WinRAR.0043F878
MOV EAX,WinRAR.004C4D60
CALL WinRAR.004591D8
XOR EAX,EAX
<ASCII "REMINDER">

ASCII
. H.@..
..A.. ..
```

```
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              Name (label) in current module   Ctrl+N
Find references to      Name in all modules
View                    Command                          Ctrl+F
Copy to executable      Sequence of commands             Ctrl+S
Analysis                Constant
```

یک نکته دیگر

اگر شما آموزش های دیگر کرکینگ باینری را نگاه کنید حتما 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 استانداردی 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 ☺