GETTING STARTED WITH IDA

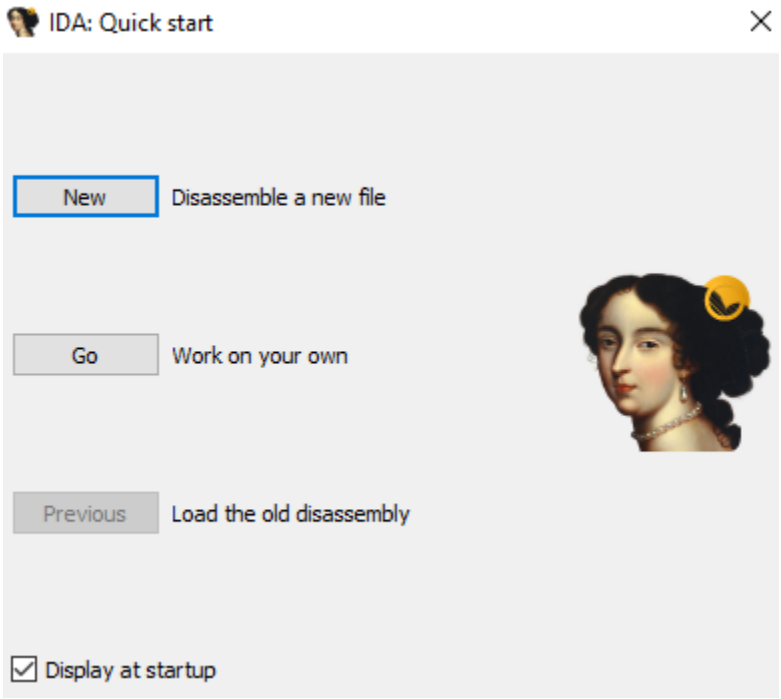
Author. Ahmad AlFareed

Section Reverse Engineering - Tools

rETKit

Launching IDA

في اي وقت تقوم بتشغيل IDA لاستخدامه سيتم الترحيب بك لفترة قليلة من خلال الشاشة البداية لـ IDA وتعرض ايضا ملخصا لمعلومات الترخيص الخاص بك. بعد هاذي الشاشة تعرض IDA مربع اخر يقدم ثلاث طرق متابعة :



اذا كنت لا تريد عرض نافذة الترحيب فقط كل ما عليك هو Display at startup ان تلغي التحديد عليه حتى يكون فارغ. يمكنك اعادة ارجاعها عن طريق اعادة قيمة 1 الى DisplayWelcome وهي تكون في Registry في مسار " Computer\HKEY_CURRENT_USER\SOFTWARE\Hex-Rays\IDA " .

الـ New يقوم بفتح نافذة explorer.exe لاختيار الثنائي المراد تحليله وبعد تحديد الملف يظهر لك نافذة اخرى في IDA يوجد بها تفاصيل اخرى سنشرحها . الـ Go يقوم بفتح IDA بدون شيء حتى ان اردت ان تسقط الملف يمكنك بدون فتح explorer.exe او استخدام خيار File لاختيار الملف. "File->Open" . الـ Previous يحدد اخر ثنائي قمت بفتحه في

IDA الحد الاقصى لهاذي الملفات 10 لكن يمكنك تغيره من خلال ملف idagui.cfg .

C:\Program Files\IDA Freeware 8.3\cfg\idagui.cfg - Sublime Text (UNREGISTERED)

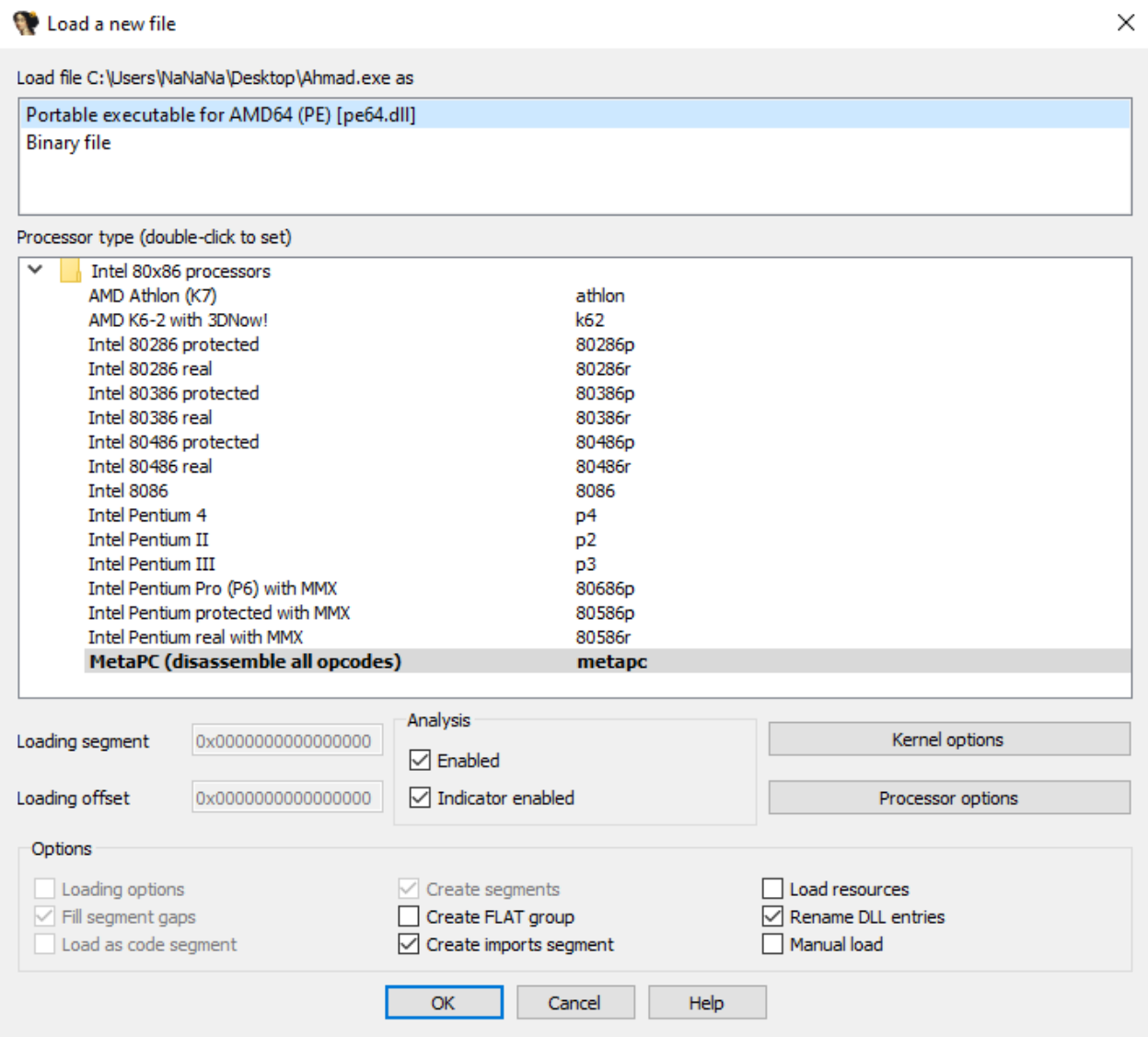
File Edit Selection Find View Goto Tools Project Preferences Help

idagui.cfg

```
1
2   //      Config file for the graphical mode user interface
3   //      ************************************************
4
5   AUTOSAVE                = 100           // After 100 user actions
6                                           // IDA flushes its buffers to disk
7
8   ASK_EXIT_UNPACKED       = YES           // Ask confirmation if the user
9                                           // wants to exit the database without
10                                          // packing it
11
12  ASK_EXIT                = YES           // Ask confirmation if the user
13                                          // wants to exit
14
15  OPEN_DEFAULT_IDC_PATH   = NO            // YES: The dialog box to select an
16                                          //      IDC script always starts in
17                                          //      the IDC subdirectory
18                                          // NO:  The dialog box opens in the
19                                          //      current/last directory
20
21  DISPLAY_COMMAND_LINE     = YES          // Display the expressions/IDC command line
22                                          // To turn on/off the command line,
23                                          // right click on the main toolbar after
24                                          // setting this parameter to YES
25
26  RECENT_SCRIPTS_MODAL    = NO            // Open "Recent scripts" window as a modal window
27
28  #define CONFIRM_UNDEFINE_NO     -1      // Never confirm
29  #define CONFIRM_UNDEFINE_YES     0      // Always confirm
30  #define CONFIRM_UNDEFINE_BLOCK   1      // Confirm only if an area has been selected
31
32  CONFIRM_UNDEFINE_COMMAND = CONFIRM_UNDEFINE_NO  // Confirm the "undefine" command
33  CONFIRM_SETFUNCEND_COMMAND = NO         // Confirm the "set function end" command (E hotkey)
34
35  CONFIRM_DETACH_FUNC_TAIL = NO           // Confirm the "detach this function tail" command
36  CONFIRM_DELETE_SELECTED_FUNCS = NO      // Confirm the "delete selected function(s)" command
37
38  HISTORY_LENGTH          =       10      // Maximum length of file->history
39                                          // Possible value is from 1 to 100
40
```

IDA File Loading

عند اختيار فتح ملف جديد باستخدام امر File Open سيظهر لك loading dialog هكذا :



تظهر لك بـ file types المحتملة وتعرض لك هاذي القائمة اعلى شيء تمثل هاذي القائمة الـ IDA loaders الاكثر ملائمة للتعامل مع هذا الملف. لاحظ انه pe64.dll (PE FOR AMD64) هذا الاصدار المجاني لا يوجد به Loaders كثير فقط الاساسية اما عند الاصدارات المدفوعة سيظهر لك MSDOS ايضا سواء اختيار هذا او هذا الخ ليس بالضرورة اختيار الاختيار الافتراضي لـ IDA يمكنك اختيار المناسب لك بناء على معلوماتك. وايضا تأكد باختيار الـ Processor Type المناسب لك. الـ Processor Type تحدد الـ processor module اثناء عملية التفكيك في معظم الحالات ستختار IDA المعالج المناسب بناء على المعلومات في الـ file's headers . عندما IDA لا تتمكن من تحديد نوع المعالج المرتبط بالملف فستحتاج الى تحديد نوع المعالج يدويا قبل . الـ Loading Segment و Loading Offset يتم تنشيط هاذي الخيارات فقط عند اختيار الـ Binary File input format الـ binary loader غير قادر على استخراج الـ memory layout انت تقوم ببناءه يدويا تقوم بوضع الـ segment and offset values لتكوين الـ base address .

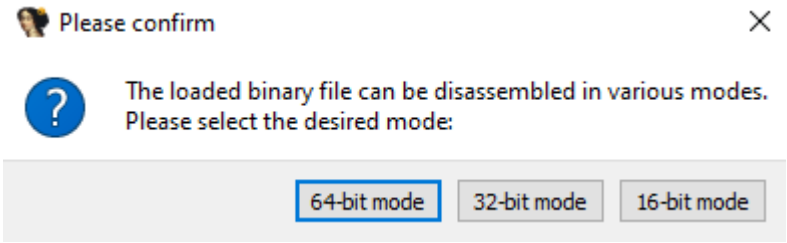
مثال على ذالك :

(Loading Offset = 0x2100,Loading Segment = 0x1000 := First Byte = 1000:2100) .

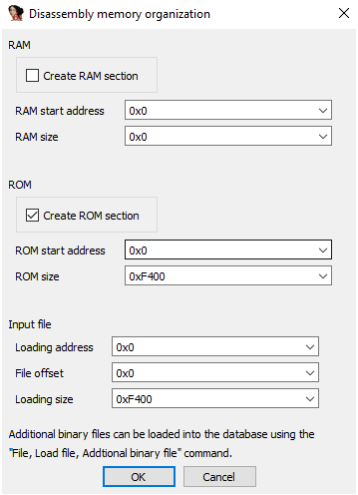
الـ Kernel Options توفر امكانية access على configure الخيارات التفكيكه الخاصه في IDA لتحسين الـ recursive-descent process التعديل والتغير يعتمد عليك لكن IDA توفر افتراضيا افضل الاعدادات لك. الـ Processor Options يوفر لك access على الـ configuration التي تنطبق على processor module المحدد. الـ Options checkboxes توفر لك تحكم افضل في التحكم بـ file-loading .

Using The Binary File Loader

عندما تختار الـ binary loader يجب ان تكون مستعد للقيام بمزيد من العمل الـ Processing . لما ما يكون في file header information لتوجيه analysis process فان الامر متروك لك للتدخل وتنفيذ المهام التي غالبا ما تقوم بها الـ loaders . امثله على ذالك تتطلب binary loader مثل الـ exploit payloads & rom images التي على الاغلب يتم استخراجها من network packet او log files . بعد اختيار Binary Loader و بدء التفكيك سيظهر لك Box :



ان لم يكن file headers لمساعدة IDA بمعرفة الملف سيتم عرض يجب التعامل مع الملف كـ 16 or 32 or 64-bit . لا تحتوي الملفات الثنائية على اي معلومات بتخطيط الذاكرة الخاصة بها على الاقل لا توجد معلومات تعرف IDA من خلالها . عند تحديد يجب تحديد الـ base address في حقلي الـ (Loading Offset & Loading Segment) . للمعالجات الاخرى غير x86 يظهر لك memory layout dialog لتنظيم الذاكرة مثل هكذا :



IDA Database Files

عند البدء في التحليل ينتج عن ذالك IDA database يتم تخزين مكوناتها في اربع ملفات (.id0, .id1, .nam, and .til) الـ .id0 يحتوي على B-tree–style database بينما .id1 يحتوي على flags تصف كل بايت في البرنامج الـ .nam يحتوي على index information مثل المواقع المسماه في Names window . اما الـ .til لتخزين المعلومات المتعلقة بتعريفات local type بقاعدة معينه. الملفات هاي فقط خاصة بـ IDA لا يمكن تحريرها في بسهولة خارج IDA . وايضا للراحة يتم ارشفة كل هاذي الملفات في ملف واحد idb. عند اغلاق IDA بشكل صحيح يجب ان لا تظهر لك الملفات التي تحتوي على ..id0 , id1 etc في المسار الخاص بك ان ظهرت لم يتم اغلاقها بشكل صحيح او تكون تالفه.

IDA Database Creation

بمجرد اختيار ملف لتحليله تبدأ IDA في انشاء قاعدة بيانات. في هذه العملية تقوم IDA بتسليم التحكم الى loader module والتي تتمثل مهمتها في تحميل الملف من القرص وتحليل اي معلومات عن الـ header قد تتعرف عليها وانشاء اقسام برنامج تحتوي على تعليمات برمجية او البيانات كما هو محدد وتحديد الـ Entry Point قبل اعادة التحكم الى IDA . الـ IDA loader modules تتصرف مثل operating system loaders . الـ IDA loader سيحدد virtual memory layout بناء على المعلومات الي في program file headers ويقوم ببناء قاعدة بيانات بناء على ذالك . بمجرد انتهاء عمل الـ loader الـ disassembly engine داخل IDA يتولى الموضوع ويبدأ بتمرير address واحد في كل مرة الى الـ processor module . وظيفة الـ processor module’s في تحديد نوع التعليمات الموجودة في ذالك العنوان وطول التعليمات في ذالك العنوان والموقع والتي يمكن ان يستمر فيها التنفيذ من هذا العنوان مثل هاذي تعليمات فرعية ام متسلسلة (sequential or branching). عندما تشعر IDA بانها عثرت على جميع التعليمات الموجودة في الملف فانها تقوم مرة اخرى عبر قائمة عناوين وتطلب من processor module لانشاء اصدار الـ assembly language version لكل instruction ليعرضها. بعد هذا التفكيك تقوم IDA تلقائيا باجراء تحليل اضافي للثنائي لاستخراج معلومات اضافية من المحتمل انها تكون مفيدة للمحلل. بمجرد الـ IDA الانتهاء من عملها والعثور على كل المعلومات او بعضها في قاعدة البيانات من تحليلها الاول :

Compiler identification

غالبا ما يكون مفيد معرفة الـ Compiler الذي تم استخدامه لانشاء البرنامج. ممكن يساعدنا في فهم الـ function calling conventions المستخدمة في binary بالاضافة الى تحديد المكتبات التي قد يرتبط بها ملف الثنائي. عندما يتم تحميل الملف تحاول IDA التعرف على الـ Compiler الذي تم استخدامه لانشاء الـ input file . اذا من الممكن التعرف على المترجم فسيتم فحص الـ input file بحثا على الـ sequences of boilerplate code المعرفة لدى هذا المترجم ويتم ترميز هذه الوظائف بالالوان لتقليل كمية التعليمات البرمجية التي تحتاج الى تحليل.

Function argument and local variable identification

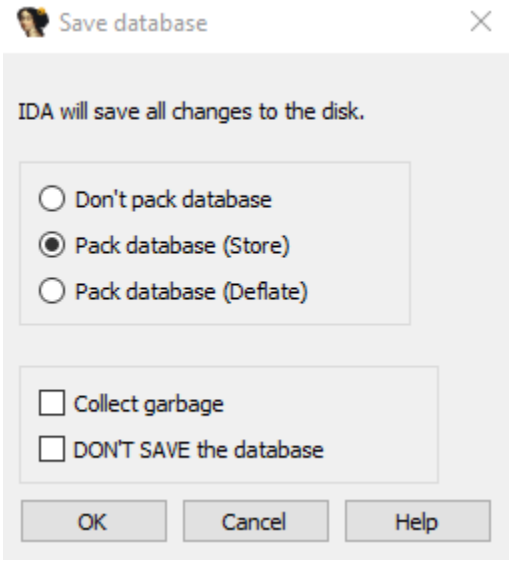
داخل كل وظيفة (call instructions) تجري IDA تحليلا تفصيليا لسلوك الـ stack pointer register من اجل التعرف على عمليات الوصول الى الـ variables الموجودة داخل الـ Stack وفهم تخطيط stack frame . الاسامي تلقائيا يتم انشاء اسامي لها اما كمتغيرات محلية او كـ arguments حصل لها passed للـ Functions كجزء من عملية الـ function call .

Datatype information

ومن خلال الاستفادة من المعرفة بالوظائف الـ library functions و required parameters تضيف IDA تعليقات الى الـ DataBase للاشارة الى المواقع التي يتم تمرير المعلمات الى هاذي الوظائف. توفر لك وقت هائل من خلال توفير المعلومات التي قد يلزم استرجاعها من application programming interface (API) references المختلفة.

Closing IDA Database

في اي وقت تقوم فيه باغلاق الـ Database سواء كنت تغلق الـ IDA بشكل كلي او تبديل الى Database مختلفة يظهر لك مربع حوار :



اذا تم انشاء قاعدة البيانات هاذي فسيتم اشتقاق اسم الملف قاعدة البيانات الجديد من input filename من طريق استبدال extension الاصلي بـ idb extension. على سبيل المثال Ahmad.exe قاعدة البيانات Ahmad.idb .
خيارات الحفظ المتاحة :

Don’t pack database

يقوم هذا الخيار ببساطة بمسح التغيرات التي تم اجراؤها على component files قاعدة البيانات الاربعة واغلاق دون انشاء ملف idb. لا ينصح بهذا الخيار عند اغلاق قاعدة البيانات الخاصة بك.

Pack database (Store)

يؤدي تحديد هذا الخيار (Store option) الى ارشفة ملفات الـ component الاربعة في ملف idb. واحد وسيتم استبدال اي idb بتأكيد. بمجرد انشاء ملف IDB يتم حذف ملفات compression الاربعة.

Pack database (Deflate)

مطابق لخيار الـ Store باستثناء ان ملفات الـ database component يتم ضغطها داخل idb.

Collect garbage

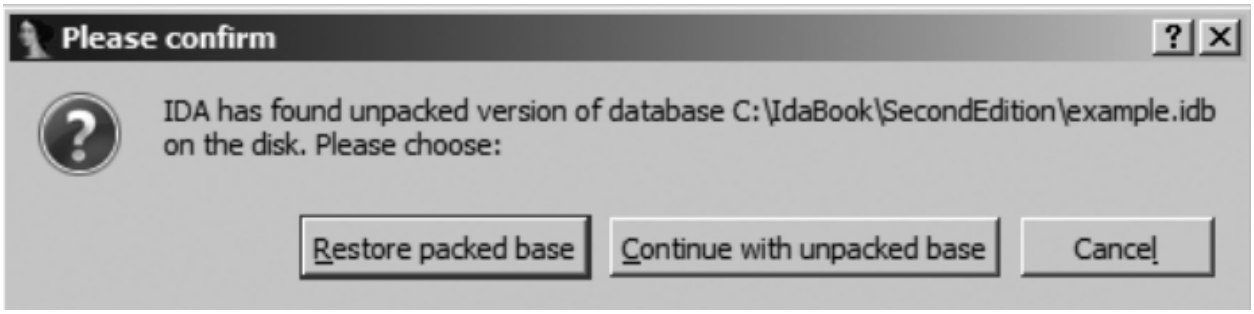
يؤدي طلب جمع القمامة او الي هي البيانات المهملة الى قيام IDA بحذف اي صفحات ذاكرة (Memory Pages) غير مستخدمة في قاعدة البيانات قبل اغلاقها. حدد هذا الخيار مع Deflate لانشاء اصغر ملف idb. ممكن.

DON'T SAVE the database

بكل اختصار لا تقم بحفظ قاعدة البيانات هذا الخيار يمكنك استخدامه لتجاهل اخر التغيرات التي قمت بها منذ اخر مرة تم حفظها فيها. بكل اختصار IDA تقوم بحذف component files وتترك IDB file موجود دون تغيير.

Reopening a Database

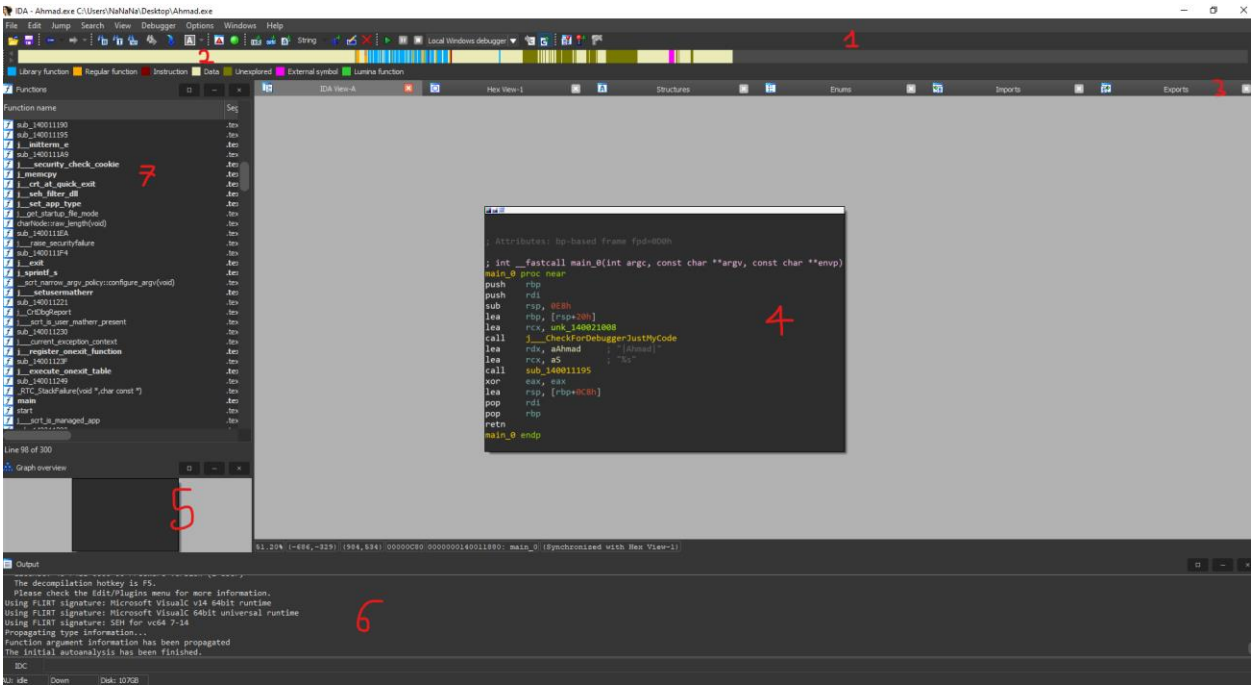
فتح الـ Database files بشكل اسرع بكثير في المره الثانية لانه لا يوجد تحليل للقيام به. كمكافأة اضافية تقوم IDA باستعادةIDA desktop الى نفس الحالة الى نفس الحالة الذي كان فيها . احيانا IDA تكرش في بعض الاحيان. سواء كان خطأ في IDA او بعض plugin التي قمت بتثبيتها . بمجرد اعادة تشغيل IDA ومحاولة فتح database الخربانة فمن المحتمل ان ترى احد المربعات مثل :



سيعرض عليك عدة خيارات ممكن ان يكون idb تالف و او الملفات الوسيطة .

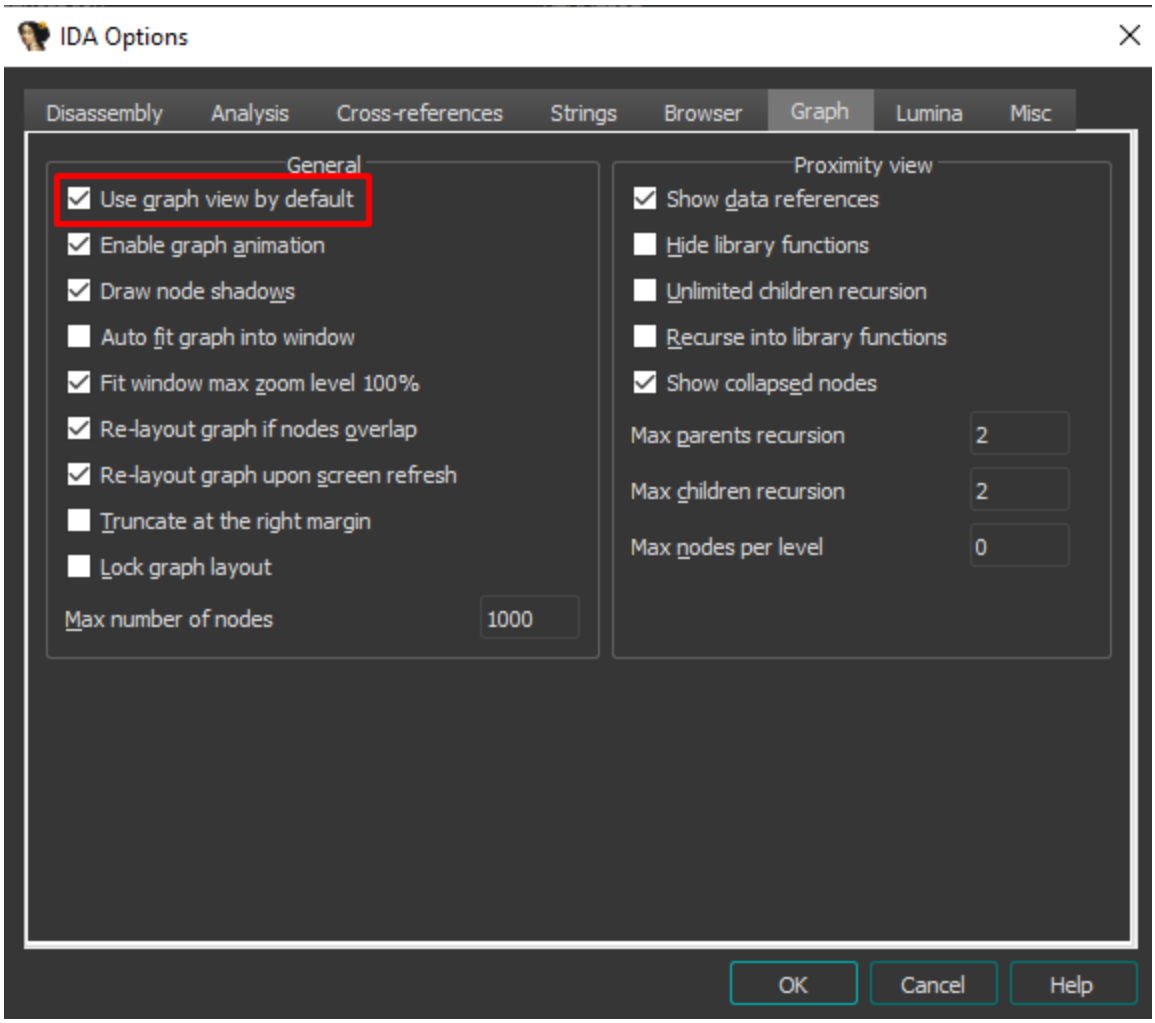
Introduction to The IDA Database

تحتاج الى القضاء ببعض الوقت في التعرف على مكونات IDA .



ستتم المناقشة اثناء التحليل لكن دعونا نشرح الارقام :

1. تحتوي منطقة شريط الادوات (toolbar area) على tools corresponding للعمليات الاكثر استخداما في IDA . تمت اضافة شريط الادوات (Toolbars) في View->Toolbars . الصورة هاذي تظهر لك basic mode toolbar صف واحد فقط من tool buttons . يتوفر الـ advanced mode "View->Toolbars->Show All".
2. الـ horizontal color هو overview navigator بمعنى متصفح النظرة العامة ويسمى ايضا navigation band الـ navigation band يقدم عرضا خطيا لـ address space للملف الذي تم تحميله. افتراضيا يتم تمثيل نطاق العناوين الكامل للملف الثنائي. يمكنك عمل zoom من خلال النقر على زر اليمين في الماوس . الالوان المختلفة انوعا مختلفة من محتوى الملف مثل البيانات او التعليمات البرمجية. يؤدي تحريك الماوس فوق احد هاذي الالوان باعطائك تلميح حوله. ويؤدي النقر الى احد الالوان الى نقلك الى مكانه ويعطيك disassembly view . يمكنك تخصيص الالوان الـ navigation band من خلال "Options->Colors".
3. الـ Data displays تحتوي على معلومات مستخرجة من الملف الثنائي وتمثل وجهات نظر مختلفة في قاعدة البيانات. ممكن ان تكون غالبية اعمالك التحليلية من خلال التفاعل مع data displays . مثل الـ IDA-View والـ Imports . يوجد عروض بيانات اخرى يمكنك استكشافها هنا "View->Open Subviews menu".
4. الـ disassembly view هو عرض البيانات الاساسي يتوفر نمطان لـ disassembly view الـ graph view (default) و listing view . في الـ graph view يعرض IDA رسما بيانيا على شكل flowchart-style لوظيفة واحدة في اي وقت . عندما يتم ذالك يمكنك الحصول على فهم لتدفق الوظيفة باستخدام التحليل البصري لـ function's structure . عندما تكون في نافذة IDA-View عند الضغط على المسافة (spacebar) يمكنك التبديل بين وضع graph view او listing . ان كنت تريد تغيرها افتراضيا يمكنك تغيرها عن طريق "Options->General menu" .



5. الـ **graph overview** تظهر فقط في حال كان نشط. هي توفر **snapshot** لـ **graph structure** . يؤدي النقر داخلها الى تغير موضع عرض الرسم البياني.
6. الـ **Output window** هي المكان الذي يمكنك ان تتوقع فيه العثور على اي رسائل من **IDA** . ستجد هنا الـ **status messages** المتعلقة بتحليل الملف او اي خطأ نتج .
7. الـ **Functions window** فيها الوظائف .

Desktop Behavior During Initial Analysis

يحدث قدر هائل من النشاط داخل الـ **IDA** اثناء التحليل التلقائي الاولي للملف المفتوح حاليا. يمكنك فهم هذا التحليل من خلال مراقبة **desktop displays** اثناء عملية التحليل . يتضمن نشاط :

- الرسائل الظاهرة في **Output window** .
- الموقع الاولي ومخرجات التفكيك يمكنك ملاحظتها في **disassembly window** .
- التحديث الدور في **Functions window** .
- تحويل نطاق التنقل في **IDA** من خلال التعرف على مناطق جديدة من الملف الثنائي كـ البيانات و والتعليمات البرمجية.

يمثل الاخراج التالي للرسائل التي تم انشاؤها من IDA اثناء التحليل الاولي للملف المفتوح حديثا. لاحظ ان الرسائل تشكل سردا للعملية التحليل ونظرة ثاقبة.

```
Loading processor module C:\Program Files\IDA Freeware 8.3\procs\pc64.dll for metapc...Initializing processor module metapc...OK
Autoanalysis subsystem has been initialized.
Loading file 'C:\Users\NaNaNa\Desktop\Ahmad.exe' into database...
Detected file format: Portable executable for AMD64 (PE)
  0. Creating a new segment  (0000000140001000-0000000140011000) ... ... OK
  1. Creating a new segment  (0000000140011000-0000000140019000) ... ... OK
  2. Creating a new segment  (0000000140019000-000000014001C000) ... ... OK
  3. Creating a new segment  (000000014001C000-000000014001D000) ... ... OK
  4. Creating a new segment  (000000014001D000-0000000140020000) ... ... OK
  5. Creating a new segment  (0000000140020000-0000000140021000) ... ... OK
  6. Creating a new segment  (0000000140021000-0000000140022000) ... ... OK
  7. Creating a new segment  (0000000140022000-0000000140023000) ... ... OK
Reading imports directory...
Reading exception directory (.pdata)...
Applying fixups...
  8. Creating a new segment  (00000001400203A8-0000000140021000) ... ... OK
Plan  FLIRT signature: Microsoft VisualC v14 64bit runtime
Plan  FLIRT signature: Microsoft VisualC 64bit universal runtime
main() function at 14001126C, named "main"
Type library 'mssdk64_win7' loaded. Applying types...
Types applied to 62 names.
Plan  FLIRT signature: SEH for vc64 7-14
Marking typical code sequences...
Flushing buffers, please wait...ok
File 'C:\Users\NaNaNa\Desktop\Ahmad.exe' has been successfully loaded into the database.
```

IDA Desktop Tips and Tricks

لا تنسى View->Open Subviews كوسيلة لاستعادة عرض البيانات التي قمت بغلقها مؤخرا بدون قصد.

Windows->Reset يوفر طريقة مفيدة لاستعادة Desktop الذي كان عليه الافتراضي الى تخطيطه الاصلي.

Windows->Save Desktop لحفظ التخطيط الحالي لتكوينات سطح المكتب التي تجدها مفيدة بشكل خاص لك الـ Windows->Load Desktop لرجوع لتخطيط المحفوظ.

Options->Font لتغير الخط.