

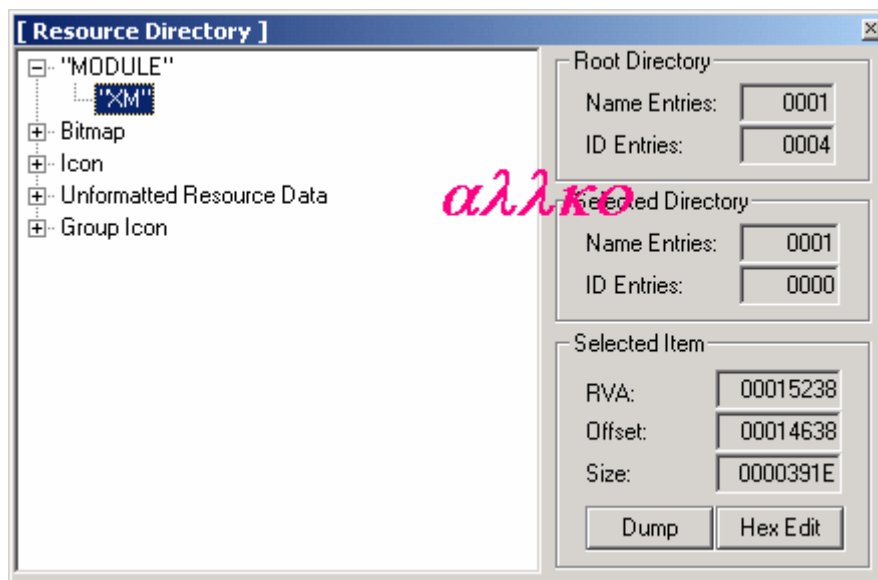
Introduction :

هذا هو آخر درس في الجزء الأول من سلسلة تعلم الهندسة العكسية... هذه هي المرة الثالثة التي اكتب فيها الدرس بسبب فقد الدرس الأصلي (بسبب موقف غبي مني في المرة الأولى وبسبب موقف أغبي من XP في المرة الثانية). سنتحدث اليوم عن كيفية استخراج الموسيقى من الملفات التنفيذية (.exe) وخاصة الـ keygens وذلك باستخدام LordPE بشكل أساسي. أتمنى أن يكون الدرس مفيدا وممتعا... أيضا أود أن أتوجه بالشكر إلى Dj-Siba و Dahaka في منتديات البرمجة والحماية، لولاهما لما كان هذا الدرس موجودا. بداية أود أن أشير أن أغلب الـ keygens تحوي الموسيقى بصيغة xm... والبعض بصيغة mod وهاتان الصيغتان تتميزان بصغر حجمهما... وغالبا يكون الملف الصوتي مضافا بهيئة resource مثله مثل الـ icons, images, dialogs, etc. وجميعها تضاف إلى قسم rsrc. من ملف الـ PE.

لمحة تاريخية:

ملفات MOD و XM تم إنشاؤها بطريقة خاصة باستخدام مزيج من الـ samples و الـ patterns للـ note data (النوتة الموسيقية). هذه الطريقة من توزيع الموسيقى تسمى tracker music. نسبة إلى البرامج التي تنشئ هذه الملفات الموسيقية مثل: (Soundtracker, Noisetraacker, Protracker, Fasttracker, Impulsetraacker, Modplug Tracker, etc) يرجع تاريخ هذه الموسيقى إلى حقبة الثمانينيات من القرن الماضي,,, واليوم فإن الـ tracker music تستخدم غالبا في الألعاب وبعض تطبيقات الأجهزة الكفية المحمولة (وبالتأكيد الـ keygens :). مما يميز هذه الملفات صغر حجمها وبالتالي فهي توفر في حجم الملف وفي الذاكرة المستخدمة من قبل البرنامج... ملفات MOD تحوي 4 قنوات موسيقية audio channels من فئة 8-bit sound. بينما الـ XM (Fasttracker) يمكن أن تحتوي عددا أكبر من القنوات الموسيقية ومن فئة 16-bit. لذلك ملفات XM أكبر حجما من ملفات MOD. يمكن تحويل كلا النوعين (MOD و XM) إلى صيغة (IT (Impulse Tracker). باستخدام برامج خاصة كـ ModPlug Tracker.

بداية افحص الملف (1) لترى انه مضغوط... إذن فك الضغط عنه مستخدما أي برنامج لفك الضغط... والآن افتح الملف الناتج باستخدام LordPE واختر Directories من القائمة اليمنى. الآن اضغط [...] بجانب Resources لترى التالي



كما ترى فإن أول قائمة بها الملف XM. اختر Hex Dump لترى التالي :

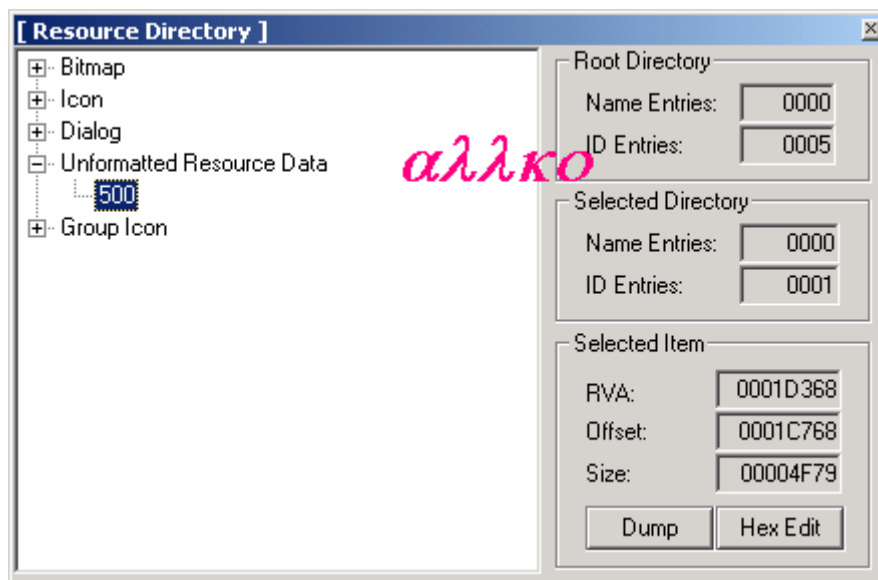
```

I.C.O.N.Extended
Module: STRANGL
EHOLD (C)JT .Fa
stTracker v2.00

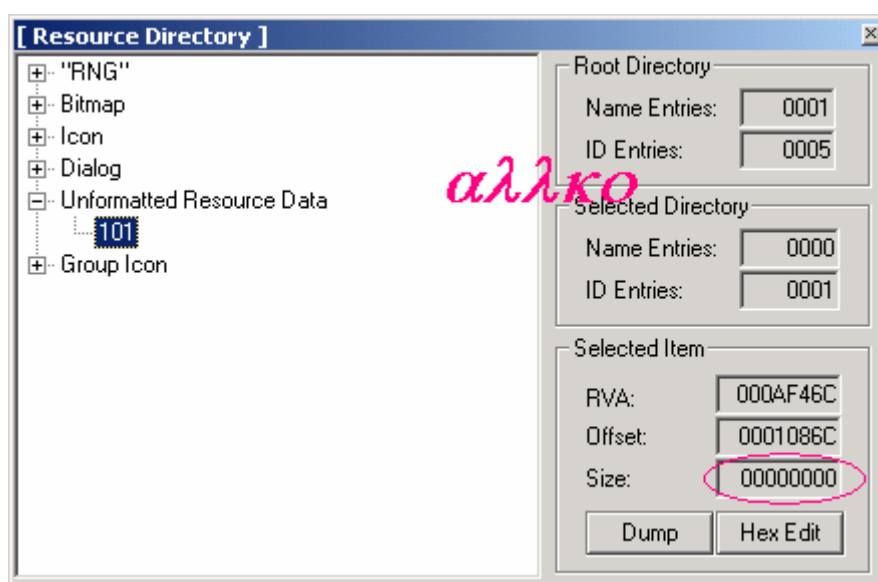
```

كما تلاحظ فإن جميع ملفات **XM** تبدأ بـ **Extended Module** . أغلق النافذة ثم اختر Dump والآن احفظ الملف بأي اسم بامتداد .xm . شغل الملف مستخدماً برنامج XMplay . ها قد انتهينا!!

يمكن تطبيق هذه الخطوات على الملفات المرفقة رقم 2 و 3 و 4 لكن لاحظ في 3 أنك ستر التالي :



لاحظ عدم وجود قائمة Module بها ملف xm كالسابق... لا بأس اختر الملف الموجود في قائمة Unformatted Resource Data ثم اختر HexDump . هل رأيت Extended Module ؟ هذا معناه أن هذا الملف عبارة عن ملف موسيقي من نوع xm . الآن كرر نفس الخطوات السابقة .
والآن دعنا نرى الملف رقم 5... فك الضغط عنه ثم افتحه بـ LordPE لترى التالي :



Unformatted Resource Data مرة أخرى... لكن هذه المرة الملف حجمه صفر كما تلاحظ... إذن ما العمل؟ افتح البرنامج باستخدام HexWorkshop والآن اضغط باليمين في أي مكان واختر Find وفي نافذة البحث اكتب Extended Module ثم انتر لترى التالي

```

00005780 0000 0000 0000 0000 0000 0000 4578 7465 .....Exte
00005790 6E64 6564 204D 6F64 756C 653A 2065 6E64 .....nded Module: end
000057A0 0000 6620 6761 656D 2020 2020 2020 2020 .....of gaem
000057B0 201A 4661 7374 5472 6163 6B65 7220 7632 .....FastTracker v2

```

والآن عرفنا بداية الملف...أما نهايته فهذه غير واضحة تماماً لكن ضع في ذهنك أن الملف الصوتي سوف يفصله عما بعده مجموعة من الأصفار.....الآن انظر إلى التالي:

```

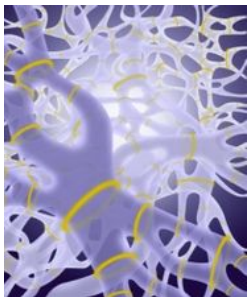
0000A850 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000A860 0000 0000 0000 0000 0000 0000 2020 2020 .....
0000A870 2020 2020 2020 2020 2020 2020 2020 2020 .....
0000A880 2020 0000 0000 0000 0000 0000 0000 0000 .....
0000A890 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000A8A0 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000A8B0 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000A8C0 0000 0000 0000 0045 6469 7400 5374 6174 .....Edit.Stat
0000A8D0 6963 0052 414E 4745 3300 0000 0000 2E3A .....ic.RANGE3.....:
0000A8E0 3A2E 2074 616D 2F43 4F52 4520 2E3A 3A2E .. tam/CORE ....
0000A8F0 0041 616E 7474 202E 2E2E 0000 0000 0000 .....About .....
0000A900 0000 0000 0000 0000 0000 0000 0000 0000 .....

```

انظر إلى ما بعد تلك الأصفار...هل يبدو لك وكأنه تابع للملف الصوتي؟ بالتأكيد لا!! يبدو وكأنه تفاصيل خاصة بالملف نفسه(الكيجن) . إذن فإن الملف الصوتي ينتهي عند تلك النقطة. إذن حدد من بداية حرف E إلى تلك النقطة و الآن اضغط باليمين على التحديد واختر copy . الآن من قائمة File اختر new ثم الآن اضغط باليمين واختر Paste ثم ok والآن احفظ الملف بأي اسم بامتداد xm واستمتع بالموسيقى.

Do You Know ?

نظرية الأوتار الفائقة :



هي مجموعة من الأفكار الحديثة حول تركيب الكون تستند إلى معادلات رياضية معقدة، تنص هذه المجموعة من الأفكار على أن الأشياء مكونة من أوتار حلقية مفتوحة متناهية في الصغر لا سمك لها و أن الوحدة البنائية الأساسية للدقائق العنصرية، من إلكترونات و بروتونات و نيوترونات و كواركات، عبارة عن أوتار حلقية من الطاقة تجعلها في حالة من عدم الاستقرار الدائم وفق تواترات مختلفة وإن هذه الأوتار تتذبذب فتصدر نغمات تتحدد وفقها طبيعة وخصائص الجسيمات الأكبر منها مثل البروتون والنيوترون والإلكترون، أهم نقطة في هذه النظرية أنها تأخذ في الحسبان كافة قوى الطبيعة: الجاذبية والكهرومغناطيسية والقوى النووية، فتوحيدها في قوة واحدة ونظرية واحدة، تسمى النظرية الأم. تهدف النظرية إلى وصف المادة على أنها حالات اهتزاز مختلفة لوتر أساسي وتحاول هذه النظرية الجمع بين ميكانيكا الكم Quantum Mechanics التي تفسر القوى الأساسية المؤثرة في عالم الصغائر (القوة النووية الضعيفة، القوة الكهرومغناطيسية، القوة النووية القوية) و بين النظرية النسبية العامة General Theory of Relativity التي تفسر قوة الجاذبية في عالم الكبار ضمن نظرية واحدة والتي تقول بأن الكون هو عالم ذو عشرة أو أحد عشر بُعداً، على خلاف الأبعاد الأربعة التي نحس بها . و أن هنالك 6 أو 7 أبعاد أخرى، إضافة لأبعاد عالمنا الثلاثة مع الزمن، غير محسوسة و متكورة على نفسها. أما هذه النظرية الجديدة فتعتقد بأن الكون مكون من 26 بعداً، أختزلت فيما بعد إلى عشرة أبعاد. ولتوضيح هذه الفكرة يستعمل البعض مثال خرطوم رش الماء، فعندما تنتظر للخرطوم من بعيد لا ترى سوى خط متعرج. لكنك بفحصه عن كثب ستري أنه عبارة عن جسم في ثلاثة أبعاد حيث أن الأبعاد الجديدة ملتفة على نفسها في جزء صغير جداً. استناداً إلى نظرية الأوتار الفائقة فإن الكون الذي نعيش فيه ليس وحيداً، وإنما هنالك أكوان عديدة متصلة ببعضها البعض، ويرى العلماء أن هذه الأكوان متداخلة ولكل كون قوانينه الخاصة به، بمعنى أن الحيز الواحد في عالمنا قد يكون مشغولاً بأكثر من جسم ولكن من عوالم مختلفة، وبحسب هذه النظرية فإن الكون ما هو إلا سيمفونية أوتار فائقة متذبذبة، فالكون عزف موسيقي ليس إلا ومن الممكن معرفة الكون ومما يتكون من خلال معرفتنا للأوتار ونغماتها، فالكون يتصرف على نمط العزف على الأوتار.

Outroduction :

A lot of thxs flyz to Dahaka and Dj-Siba coz without them this lesson couldn't see the light !

Greetings :

DiDi

Dahaka

Dj-Siba

