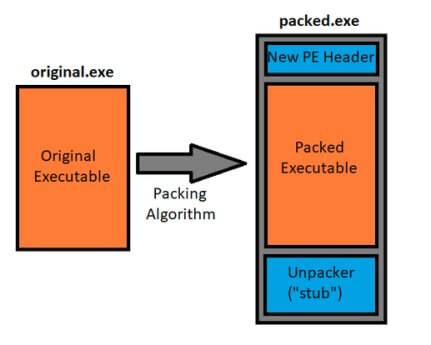
**What is a malware packer**

وش هو packer و ليش نستخدمه

**وش يعني packer**

خلني اشرح بشكل بسيط مره وش هو packing

​



​

باختصار شديد هي عمليه ضغط لملف بمعنى عندي ملف exe سواء كان malware او غيره اقدر استعمل packer عشان اضغط الملف و اذا ضغطته و حاولت اسوي له RE او هندسة عكسية ماراح يطلع لي الاسمبلي حق exe الأصلي نفس لما يكون عندك txt و تضغطة باستخدام winrar بالطريقة ذي لما تفتح الملف بعد الضغط ماتقدر تشوف محتويات ملف txt حقك, و في مرحلة التشغيل راح ينفك packer و يشتغل البرنامج طبيعي

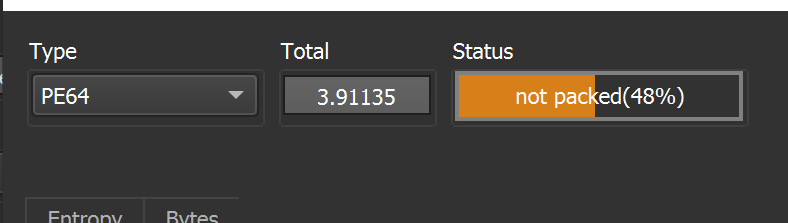
​

**وش هدف ال packer**

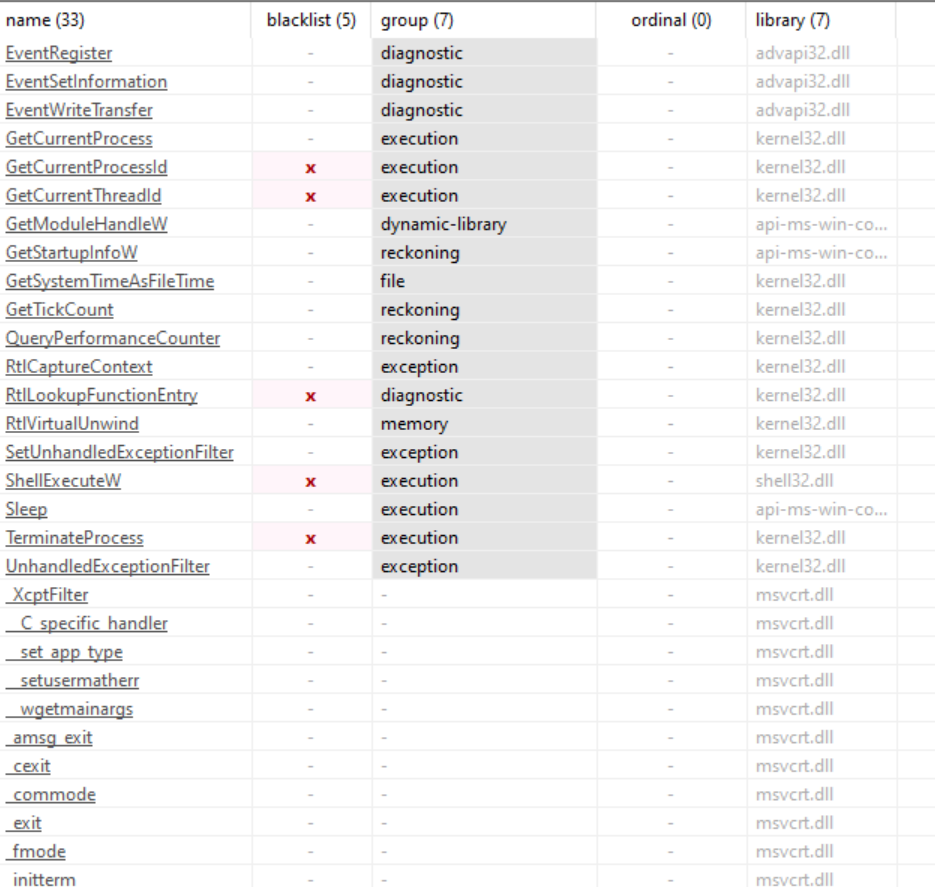
له اهداف كثير بس الهدف الرئيسي هو اني امنعك من انك تقرا الاسمبلي حق الملف حقي بصورة مباشرة و من استخداماتة ايضا هو ضغط الملفات لأن exe بعد packing يكون حجمة اصغر

**كيف نعرف ان malware حقنا packed او لا**

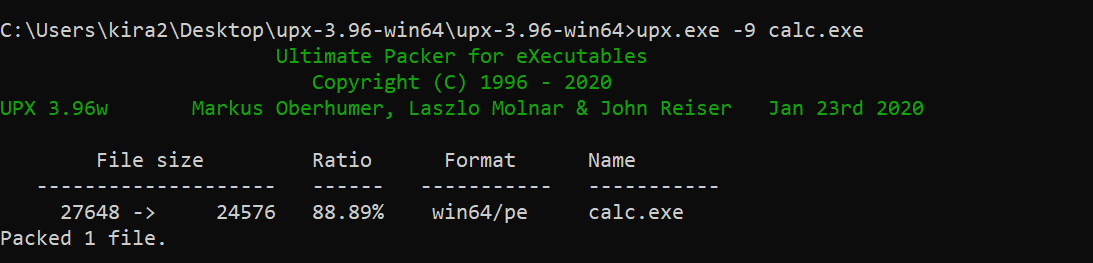
عندنا اشياء كثير ممكن نسويها من اسهلها هو Entropy و كيف يشتغل؟ اذا شاف الملف عشوائي يزيد Entropy طيب بناخذ الحين calc.exe و بنفحصها قبل ما نسوي لها pack و بعد pack و نشوف الفرق



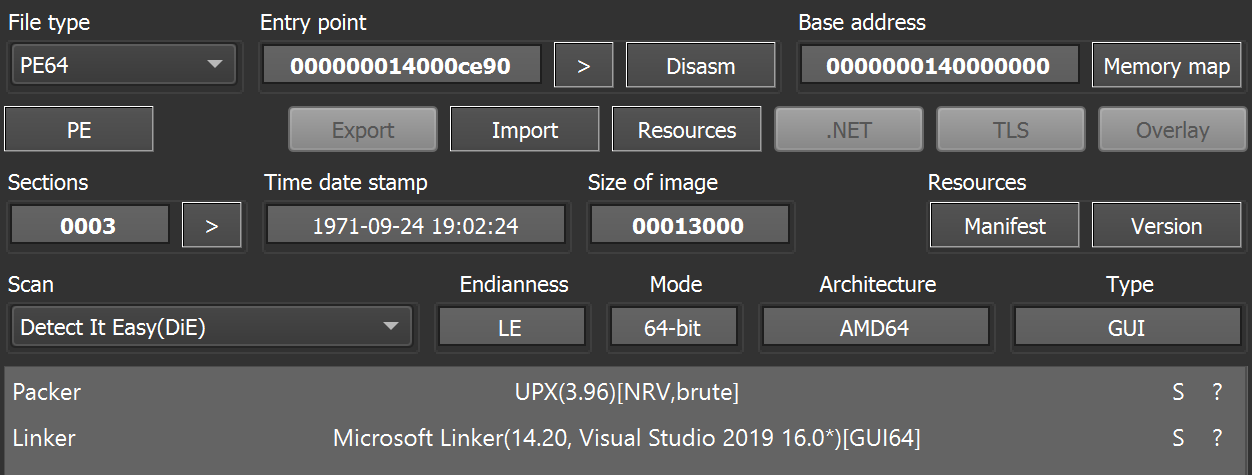
استخدمنا برنامج Detect it easy عشان نقدر نعرف Entropy حق الملف و زي ما نشوف يقول not packed



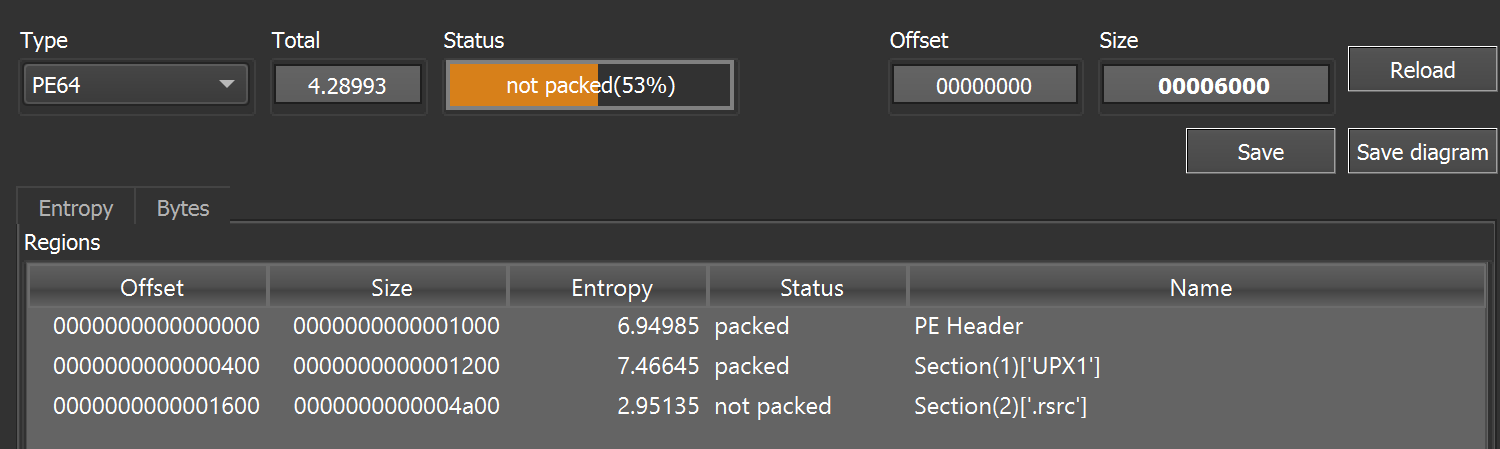
و هنا استعدملت pestudio عشان اطلع معلومات عن functions المستخدمة و نلاحظ ان functions كثير هنا ,و الحين نجرب upx و هو نوع من انواع packers و مشهور جدا



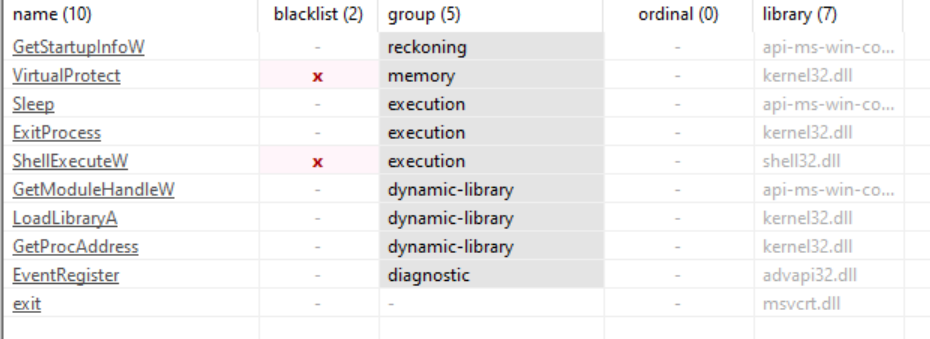
لو نلاحظ حجم الملف صار اصغر الحين بنسوي عليه نفس اللي سويناه فوق و نشوف الفرق



نقدر نشوف ان DIE تعرف على packer و عطانا اسمه و عطانا الاصدار بعد



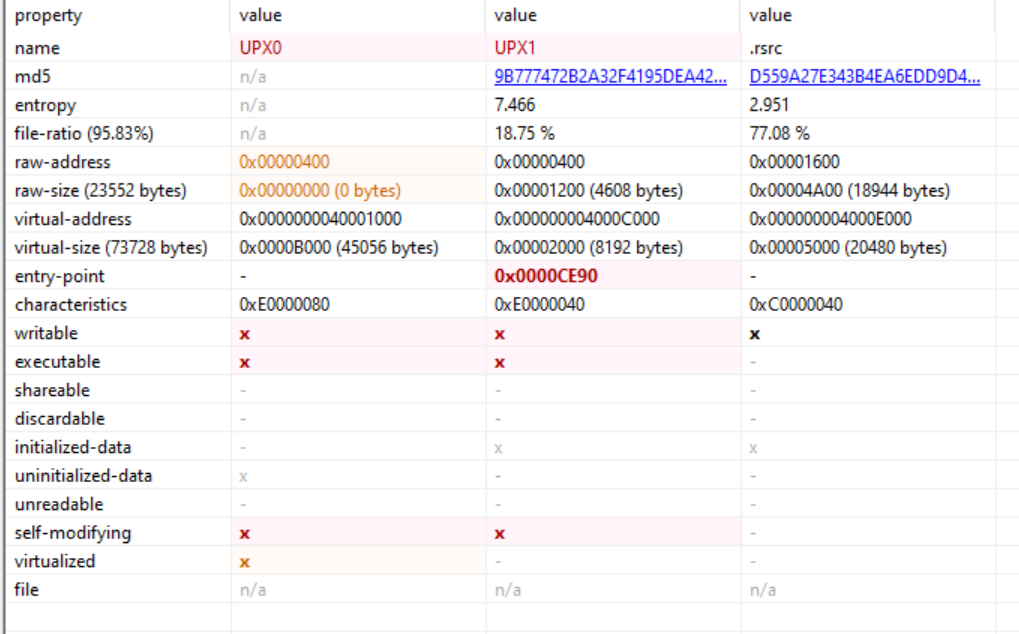
لو نشوف Entropy بنلاحظ انه not packed بس لما ننزل تحت نشوف ان فيه اشياء packed و هي sections و الحين عرفنا معلومه ان مو شرط نعتمد على Entropy حق الملف بشكل كامل لازم نشوف sections بعد



الحين لو نشوف الfunctions المستعملة ما نلاقي الا شي قليل مقارنة بقبل عملية pack بتلاقي في packed exe بعض ال functions اللي تعطيك تلميح انه packed مثل

VirtualProtect VirtualAlloc WriteProcessMemory

هذي كلها ممكن تلمح لك ان البرنامج packed



و لو نروح ل sections بنلاقي اسامي غريبه مثل UPX0 و نلاقي بعد ان فيها صلاحيات writeable و executable و هذي تخلينا نتيقن اكثر انه packed

**الملخص**

قدرنا نعرف وش pack و ليش يستخدم و كيف نعرف ان هذا packed او لا السؤال هل بس الmalware يسوي pack؟ لا حتى البرامج اللي ماتبيك تشوف السورس السورس حقها و تعرف كيف تشتغل تحطه عشان تصعب عليك هل نقدر نفكه؟ ايه نقدر نفكه طبيعي جدا و حتى اذا كان فكه صعب لازم تعرف ان packer في الاخير لازم يشغل الملف الاصلي ف لما نستخدم debugger بنقدر نشوف اكواد الكود الاصلي تشتغل بعد مايخلص من عملية unpacking

​

**مصادر**

​<https://bidouillesecurity.com/tutorial-writing-a-pe-packer-intro/> <https://upx.github.io/> <https://www.varonis.com/blog/x64dbg-unpack-malware>