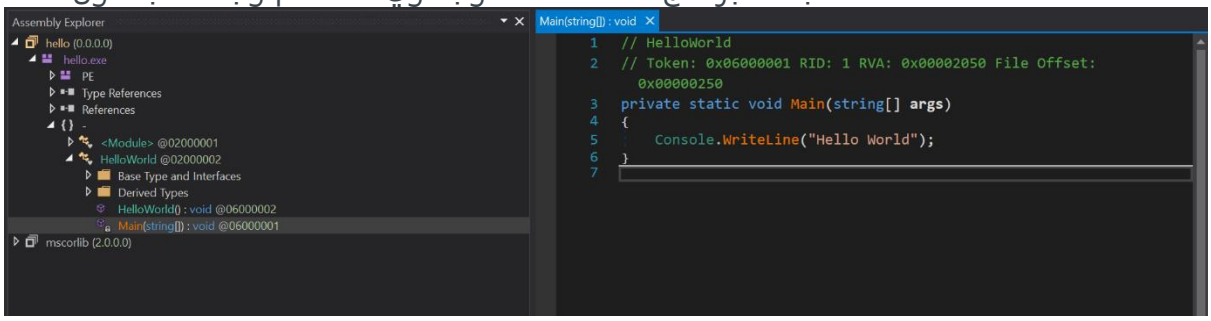
unpack csharp packer

بسم الله الرحمن الرحيم

سويت packer بسيط باستخدام csharp و الحين بشرح لكم كيف يشتغل و كيف تفكونة charp_packer

بناخذ برنامج hello world و بسوي له pack و بعدها بنحاول نفكه



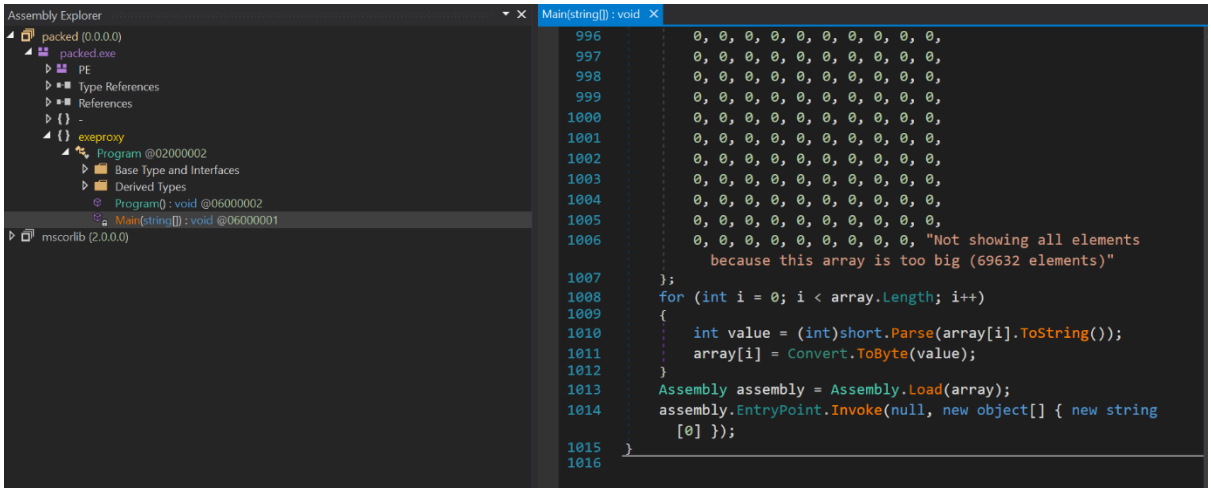
هذا هو البرنامج حقنا بس يطبع Hello World

```
Microsoft Windows [Version 10.0.19044.1766]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kira2\Desktop\ppid\packer>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\kira2\Desktop\ppid\packer> .\pack.ps1 hello.exe packed.exe 6
```

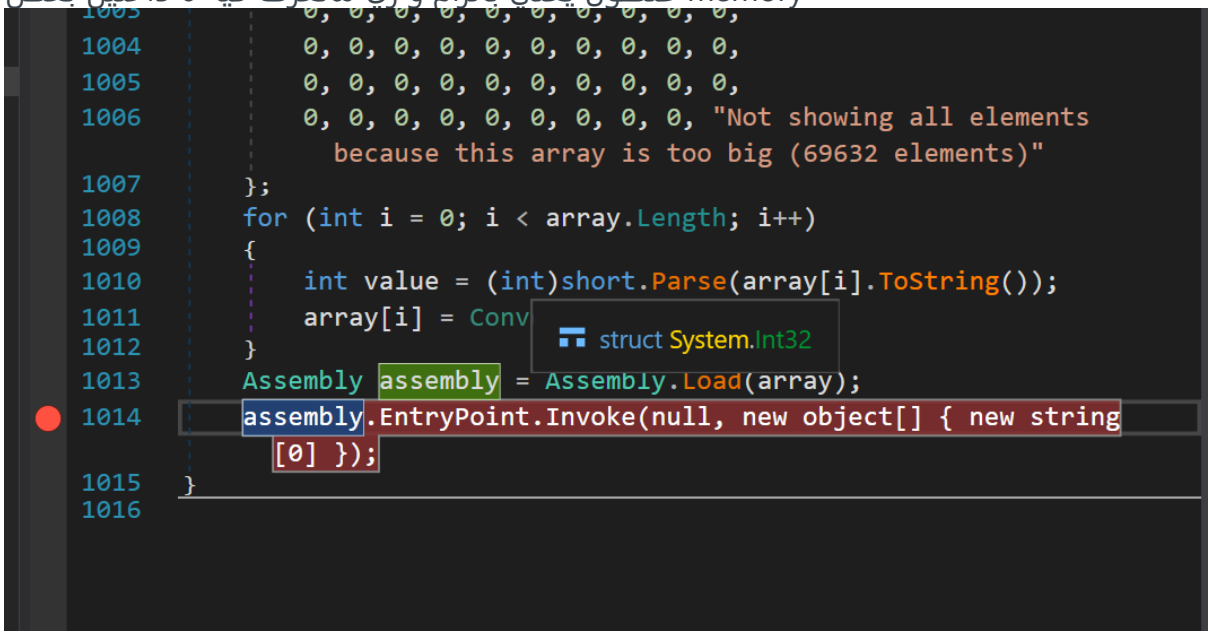
الحين بس نسوي pack نحط اسم الملف حقنا و اسمه بعد مايصير pack و رقم سته الحين بشرح لكم ليه

كيف يشتغل ال packer

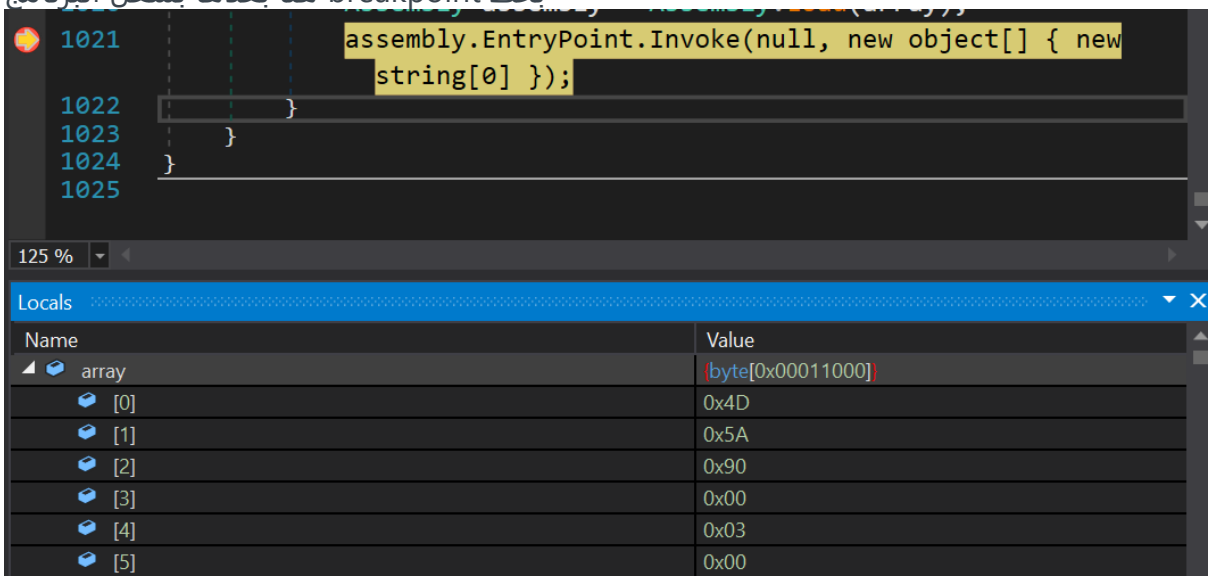
طريقة عمله هي انه ياخذ exe و يدخلة ب exe ثاني و الرقم اللي نحطه هو عدد المرات اللي يسوي الشي هذا ف بيحط exe داخل نفسه 6 مرات ليش اخترت 6؟ عشان يكون فكه ابسط كل مازاد الرقم زادت صعوبته اكثر



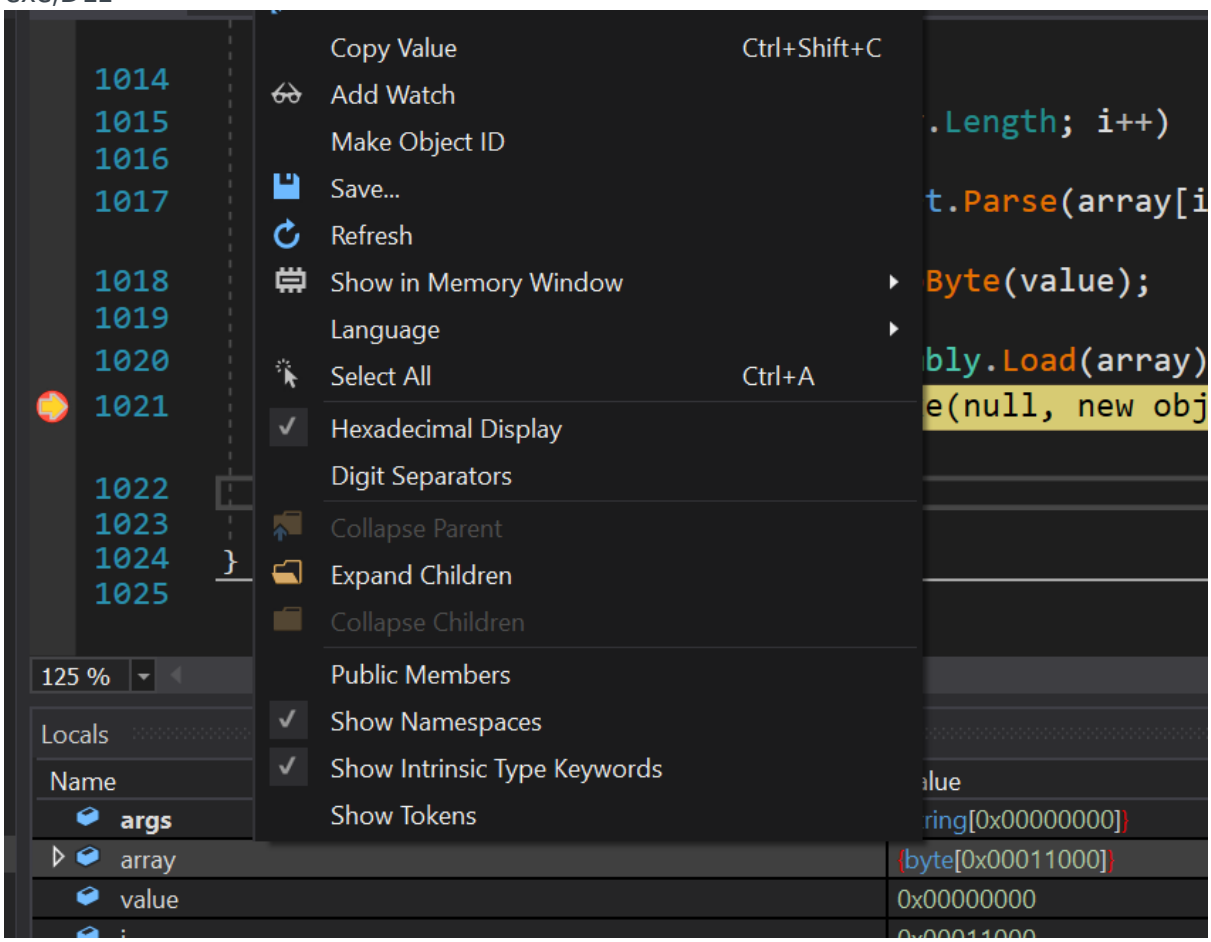
بياخذ exe و بيسوي له invoke و عشان اشرحه بطريقة بسيطة ياخذ بايتات exe و يشغلها في memory علطول يعني بالرام و زي مانعرف فيه 6 داخلين بعض



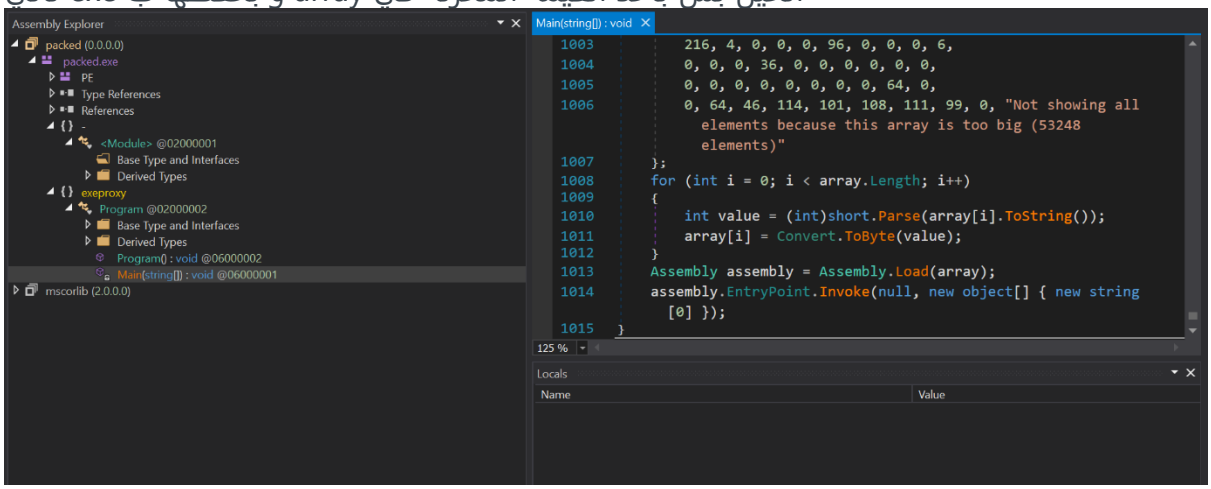
بحط breakpoint هنا بعدها بشغل البرنامج



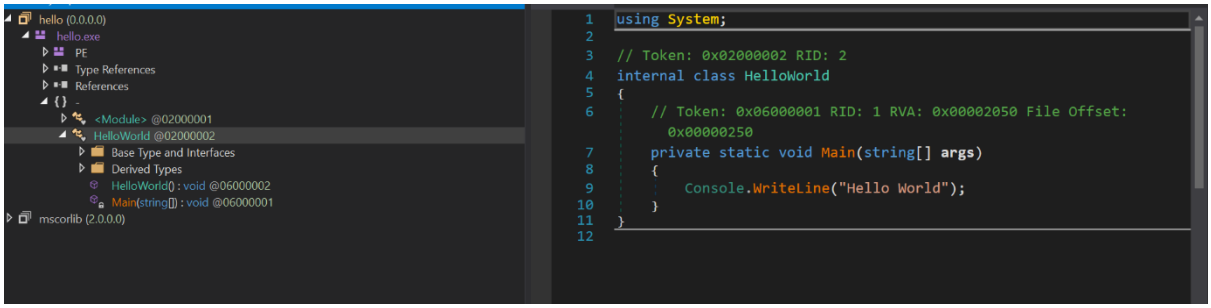
لو نلاحظ في متغير array نلاقي D5A4و هي hex و تعني MZ و هذي header حقت PE مثل exe,DLL



الحين بس باخذ القيمة المخزنة في array و بحفظها ب exe ثاني



هنا بعد ما حفظناه و حطيناه ب exe نلاحظ انه نفس اللي جانا بالملف الاول بس الفرق هو البايتات تختلف بنرجع نسوي زي اللي سويناة فوق ناخذ قيمة array بكرر العملية هذي الين يطلع معنا شي مختلف



بعد تكرار العملية 6 مرات قدرنا نرجع للكود الأصلي و الحين نقدر نحلل لو كان exe داخل نفسه 100 مره كان الموضوع بيكون اصعب و ممكن نلاقي طريقة ثانية

الملخص

كل packer بالعالم تقدر تفكة لأنه في مرحلة ما راح يفك نفسة و كثير من C# packer تقدر تفكهم نفس الطريقة اللي سويناها نحط breakpoint على المكان اللي بيفك منه و نسحب exe الاصلي بعد unpacking