2018

Reverse Engineering Tutorials Series

Simple Patching

سلسلة دروس الهندسة العكسية

الترقيع البسيط

Haboob Team

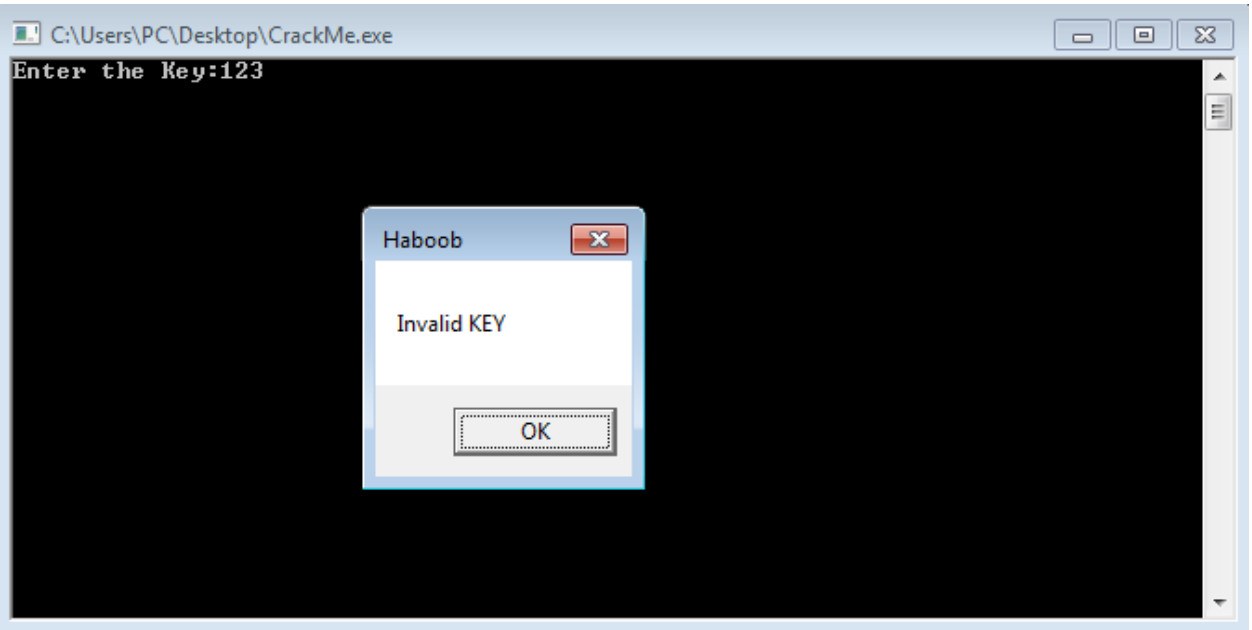
بسم الله الرحمن الرحيم

الهندسة العكسية مجال واسع وهذا الدرس مقدّم للمبتدئين حيث سيتم شرح عملية ترقيع البرامج "patching" لتخطي السيريال نمبر الخاص بالبرنامج.

قبل البدء نحتاج للبرنامج التالي: "Olly Debugger" او اي برنامج آخر يقوم بنفس الطريقة

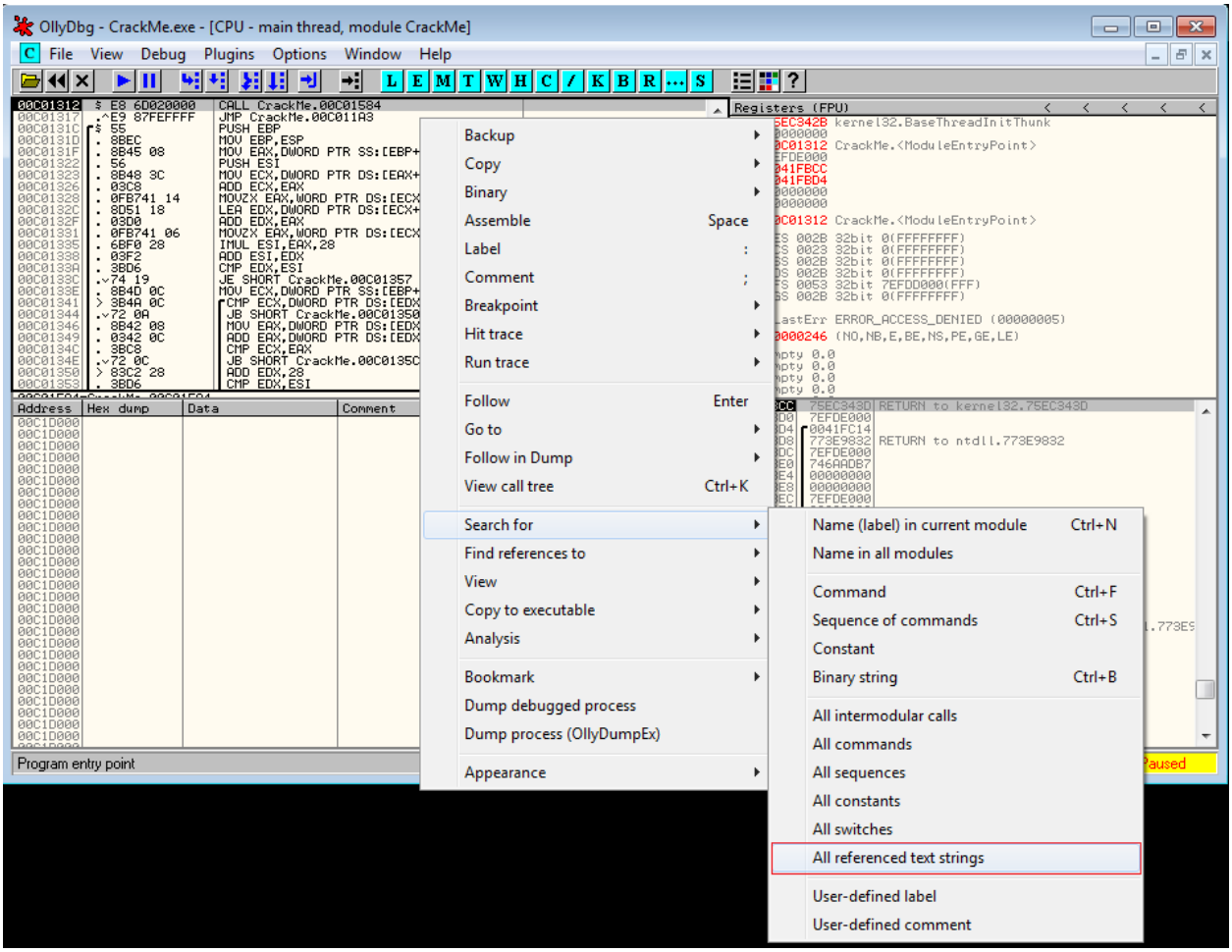
أيضاً قبل البدء, يلزم القارئ الحصول على نبذه بسيطه في لغة الاسمبلي وآلية عمل الستاك "Stack" اذا كان الهدف الإلمام بالهندسة العكسية اما اذا كان الهدف للتطبيق فقط فلا يلزم, حيث يمكن تطبيق الدرس بدون الإلمام.

تم عمل برنامج بسيط يطلب كود لتفعيل السريال نمبر بلغة السي لتطبيق الشرح, حيث يضهر البرنامج رسالة خطأ عند ادخال رقم السريال الخاطي ويتم اغلاق البرنامج ورسالة صحيحة عند ادخال الرقم الصحيح.

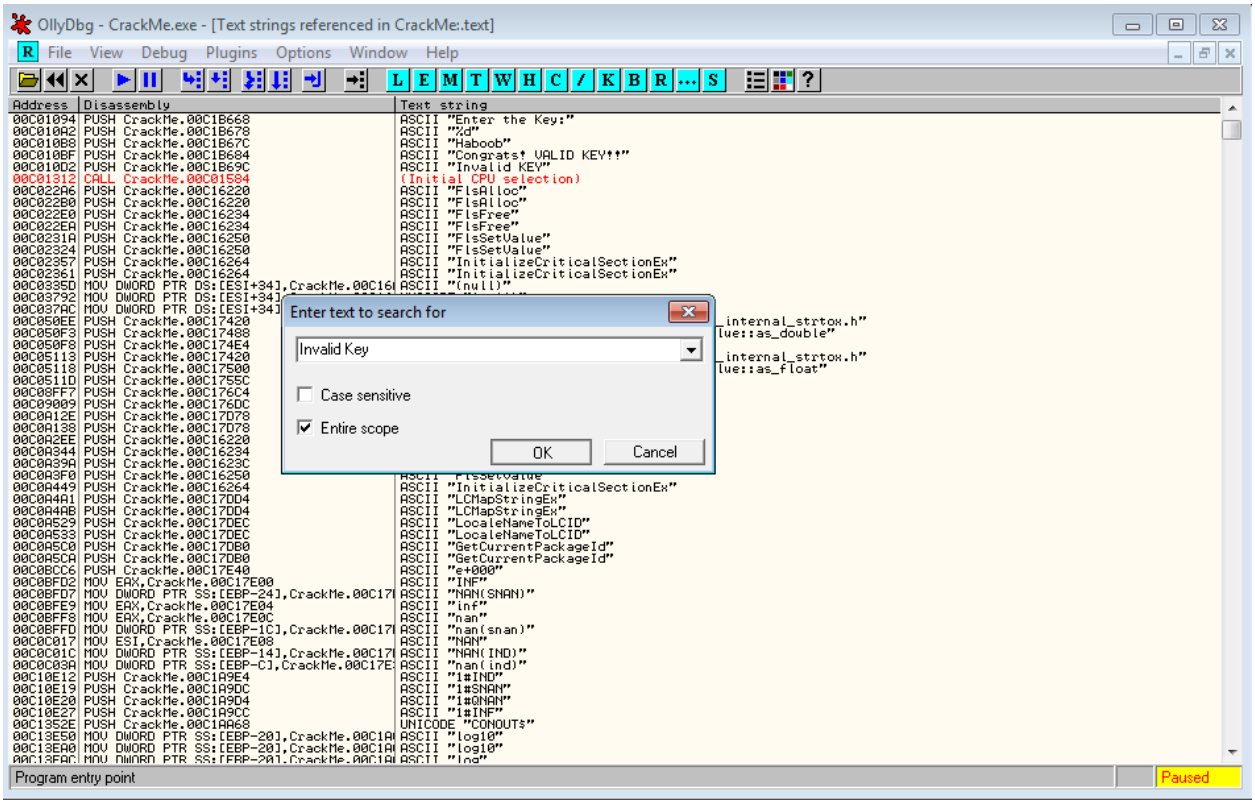


نقوم بفتح ملف الـ exe ببرنامج الـ "Olly Debugger" عن طريق الخيارات او بالضغط على مفتاح F3.
بعد فتح الملف ببرنامج الـ Olly نقوم بالضغط على زر تشغيل البرنامج او بالضغط على مفتاح F9 (لمرة واحدة فقط)

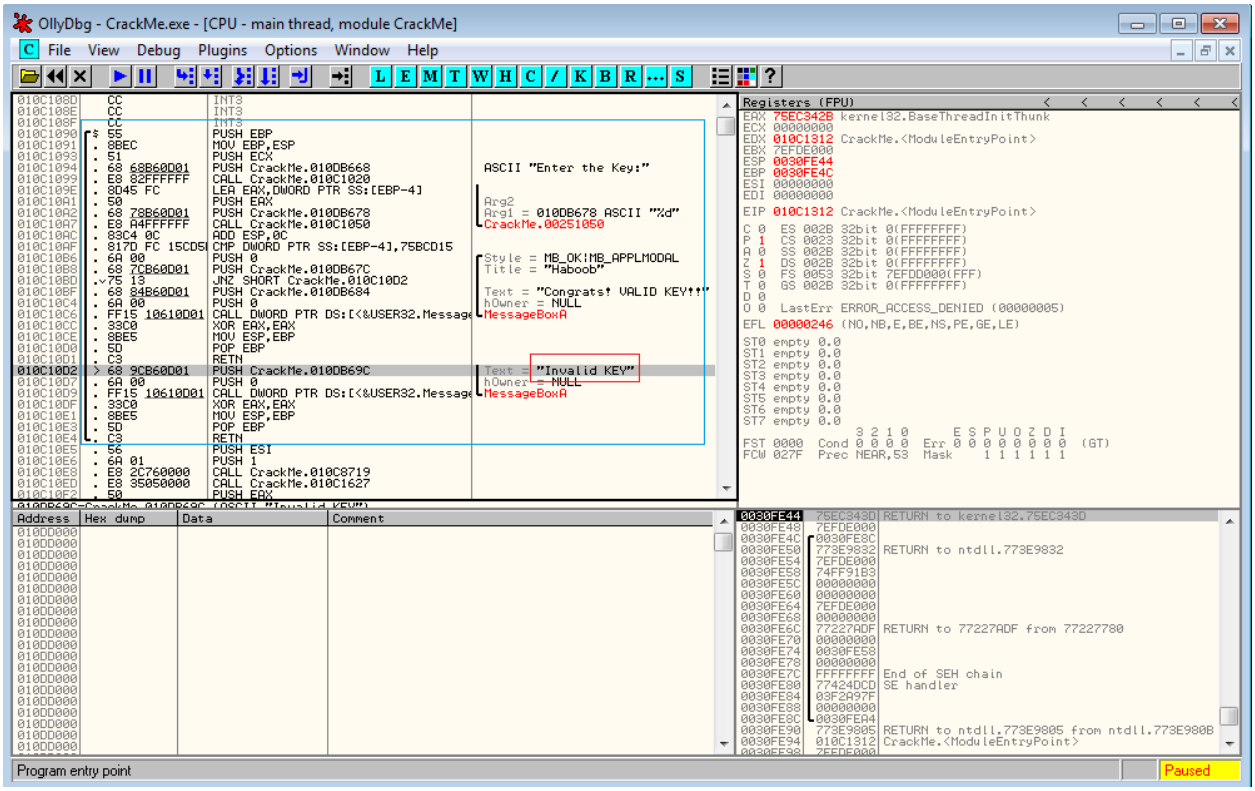
بعد ذلك نقوم بالضغط على الزر الايمن في المساحة اليسرى (المساحة الخاصة بالديساسمبلر "Disassembler") ومن ثم اختيار [Search for ➔ All referenced text Strings] كما هو موضح في الصورة.



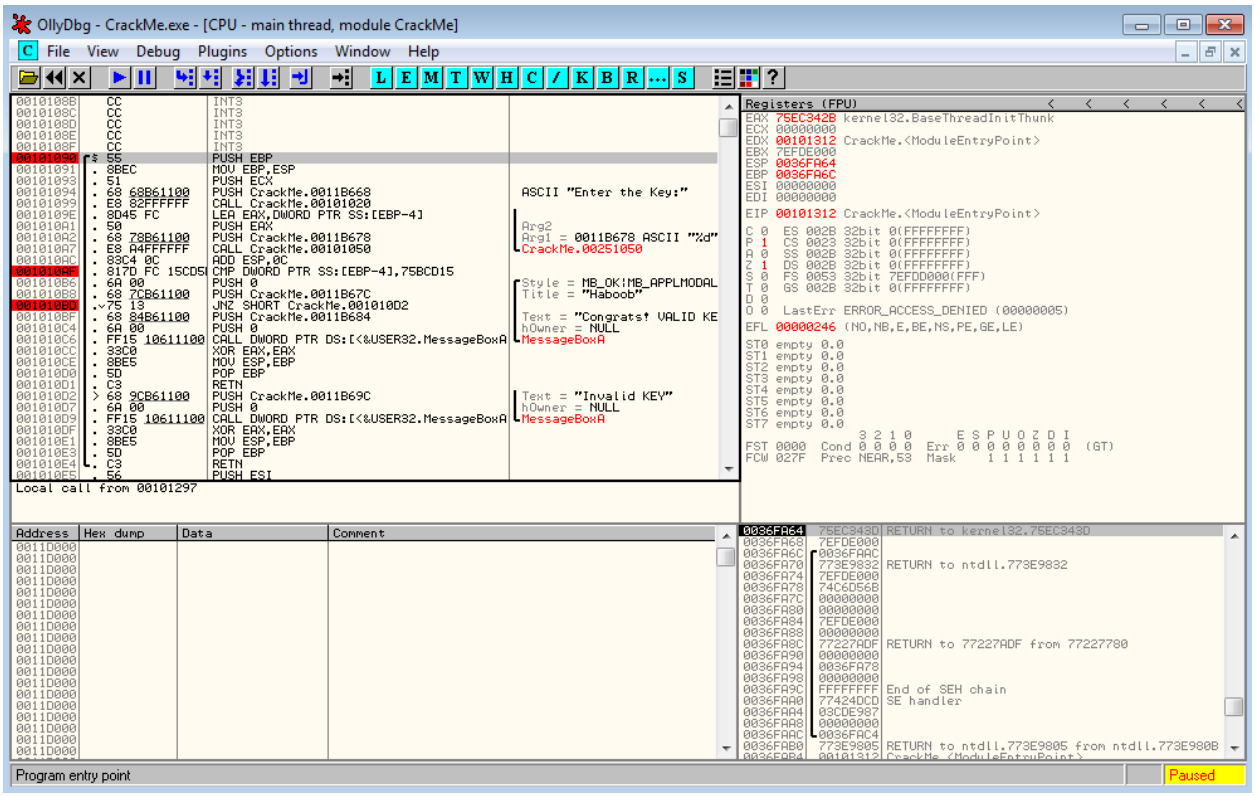
عند اختيار الخيار اعلاه سيتم الوصول الى الصفحة الخاصة بالنصوص "Strings" نقوم بالضغط على الزر الأيمن واختيار "Search for text" ثم نبحث عن رسالة الخطأ التي ظهرت عند ادخال رقم السيريال الخاطئ في أول صورة بالشرح وهي "Invalid KEY"



بعد البحث وايجاد النص يتم الضغط مرتين عليه ليتم نقلنا الى نافذة الديساسمبلر "Disassembler" كما في الصورة التالية

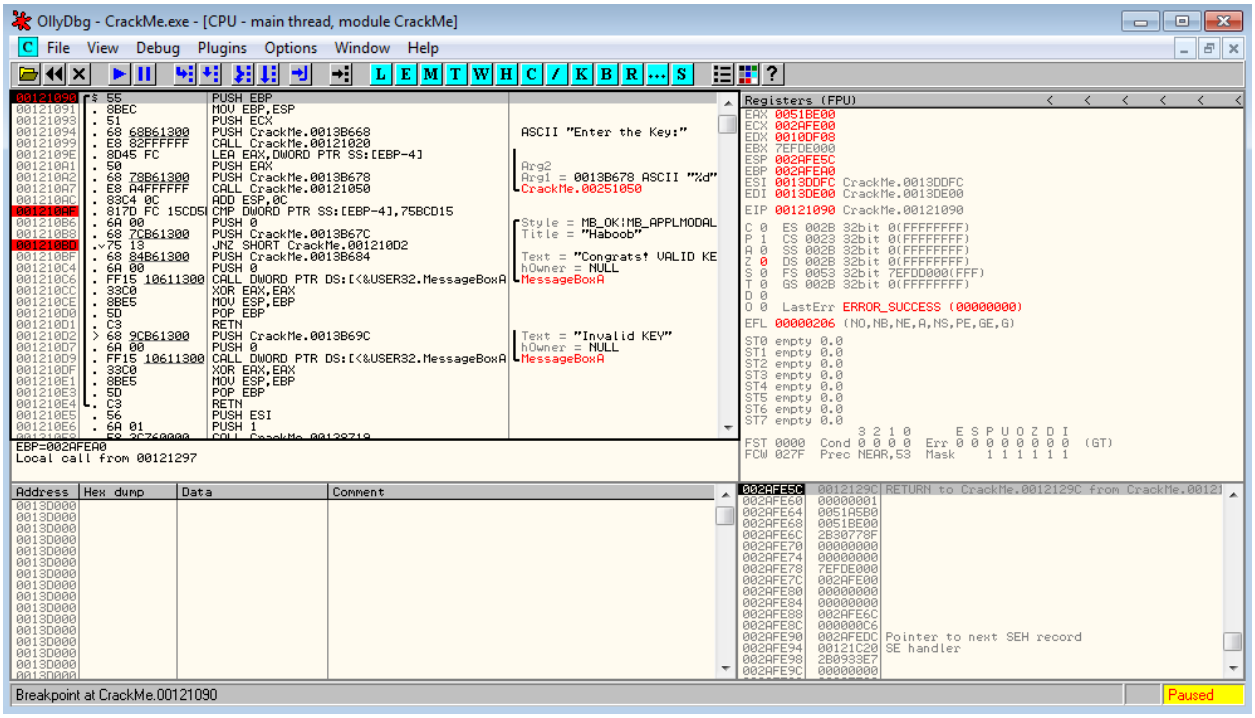


هنا نصل الى المهم, الحدود في اللون الازرق تسمى إطار الستاك "Stack Frame" وهذا مايهمّنا لعمل الترقيع للبرنامج.

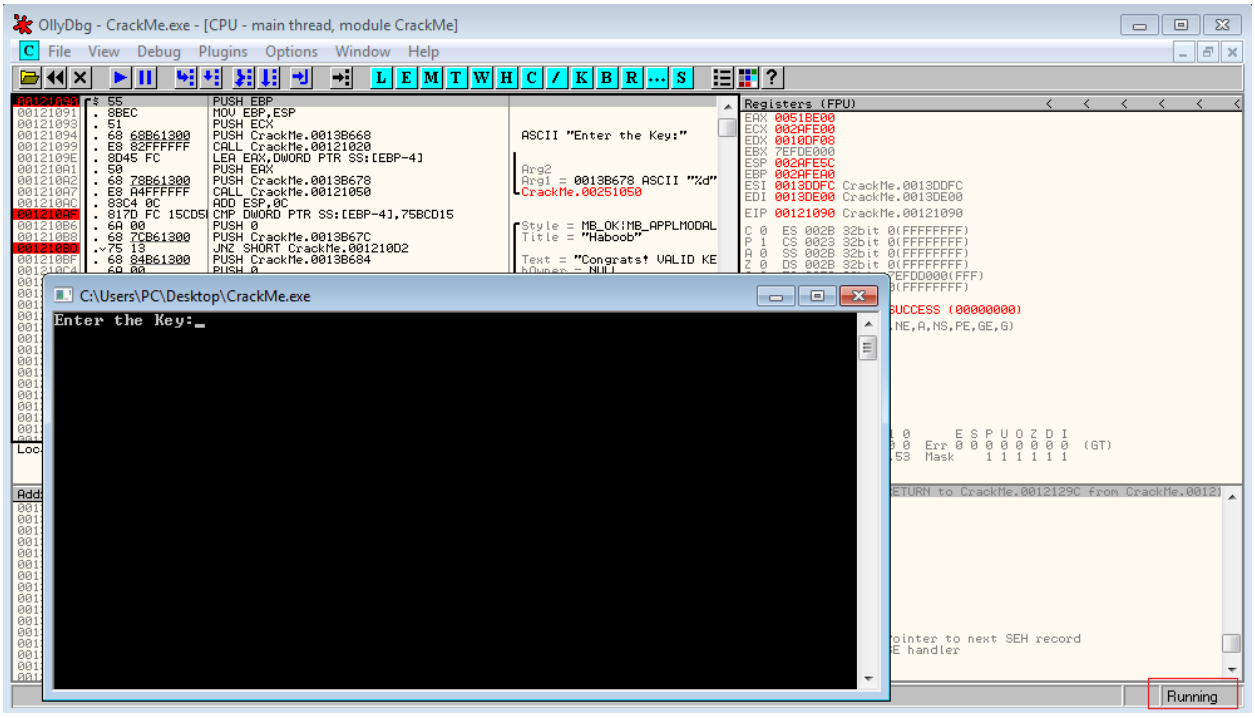


في الصورة اعلاه تم الضغط على زر الـ F2 لعمل نقطة كسر "Break Point" على بعض العمليات كما هو موضّح في اللون الأحمر في الصورة وتعني (عندما نقوم بتشغيل البرنامج يتم ايقاف البرنامج عند الوصول لأي عملية باللون باللون الأحمرالى ان يتم تشغيل البرنامج مرة أخرى بالضغط على زر F9, وهنا لن يتم التطرّق لجميع العمليات او بمصطلح آخر الأوامر (Instructions) في إطار الستاك "Stack Frame" وماتعنيه لأن الشرح خاص بالمبتدئين ونكتفي بالعمليات التي وضعنا عليها نقطة كسر "Break Point" (الموضحة باللون الأحمر على اليسار في الصورة اعلاه)

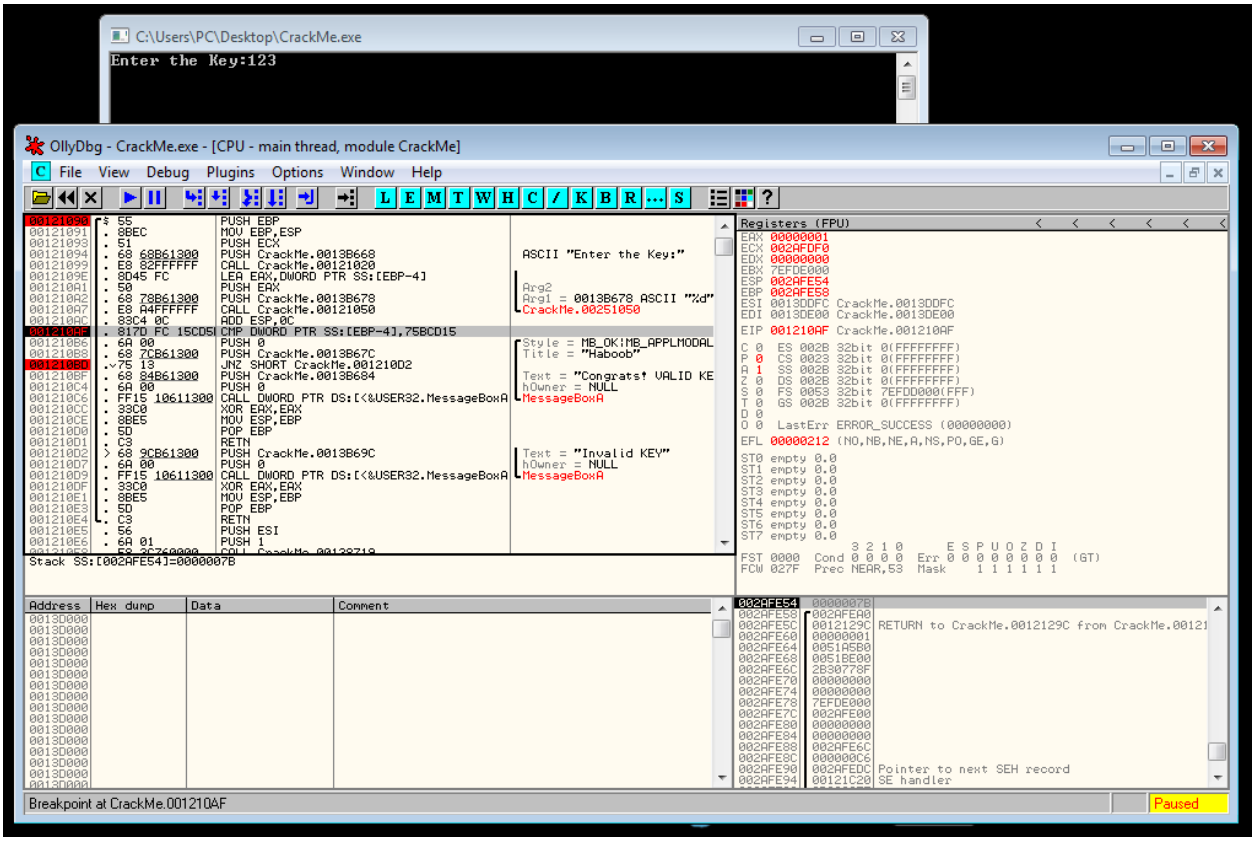
نقوم بعد تحديد العناوين والضغط على زر الـ F2 لتصبح باللون الأحمر بضغط زر التشغيل في القائمة باللون الازرق او ضغط زر الـ F9 الى ان يتم تغير اللون الاحمر للأسود كما في الصورة التالية عند هذا العنوان 00121090 وكما نلاحظ في اسفل الشاشة يمين باللون الأصفر ان البرنامج متوقف (Paused).



نقوم بعد ذلك بالضغط على زر التشغيل في البرنامج او الضغط على زر الـ F9 مرة اخرى لتخرج لنا نافذة البرنامج لإدخال الرقم (السريال نمبر) كما في الصورة التالية, أيضاً نلاحظ ان اسفل الشاشة يمين ان البرنامج في وضع التشغيل (Running).



نقوم بعد ذلك بإدخال أي قيمة كـ رقم سري في البرنامج والضغط على زر إدخال في لوحة المفاتيح للنتقل الى الصورة التالية.



كما نلاحظ في الصورة اعلاه قمنا بإدخال الرقم 123 (او أي رقم آخر) ومن ثم ضغط زر ادخال (Enter) الموجود في لوحة المفاتيح وتم توقف البرنامج كما هو موضح اسفل الصورة يمين باللون الأصفر, ووصلنا الى نقطة الكسر "Break Point" التالية في عنوان الذاكرة (001210AF).

مايهمنا الآن هما العملية الثانية والثالثة باللون الأحمر في الصورة اعلاه لنتطرق الآن لشرحهما وهم.

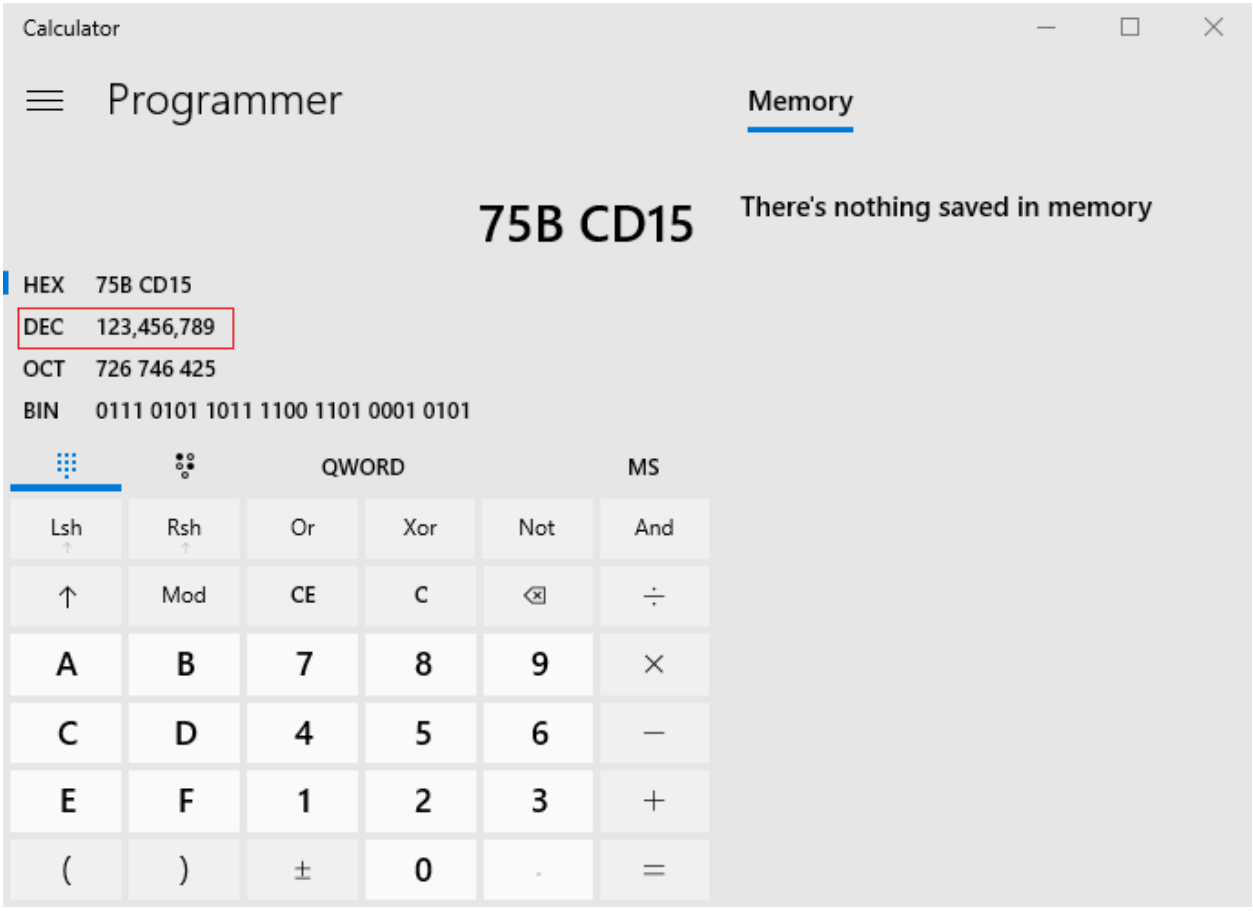
```
1. 001210AF   817D FC 15CD5B07   CMP DWORD PTR SS: [EBP-4], 75BCD15
2. 001210BD    75 13             JNZ SHORT CrackMe.001210D2
```

في العملية الثانية, عند العنوان 001010AF يتم مقارنه القيمة التي يحتويها [EBP-4] بهذه القيمة 75BCD15 :

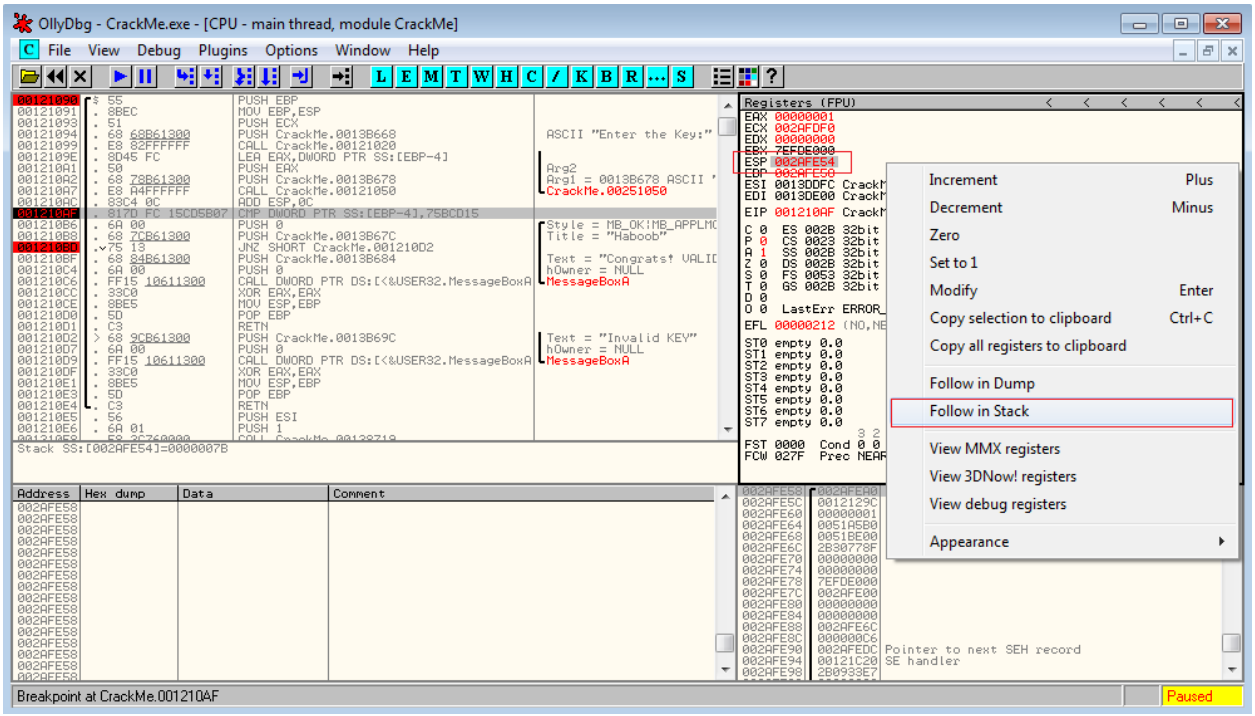
في العملية الثالثة, عند العنوان 001210BD هذه العملية عبارة عن عملية انتقال مشروط وهي اختصاراً لـ (Jump if Not Zero) وتعني:

- اذا كانت القيمة الموجوده في [EBP-4] لاتساوي هذه القيمة 75BCD15 (ملاحظة: هذه القيمة بالنظام الست عشري (hexadecimal)) سيتم الانتقال الى عنوان الذاكرة (001010D2).
- اذا كانت القيمة الموجوده في [EBP-4] تساوي هذه القيمة 75BCD15 لن يتم الانتقال الى عنوان الذاكرة (001010D2) وسيتم تنفيذ العملية التي تليها في هذا العنوان 001010BF.

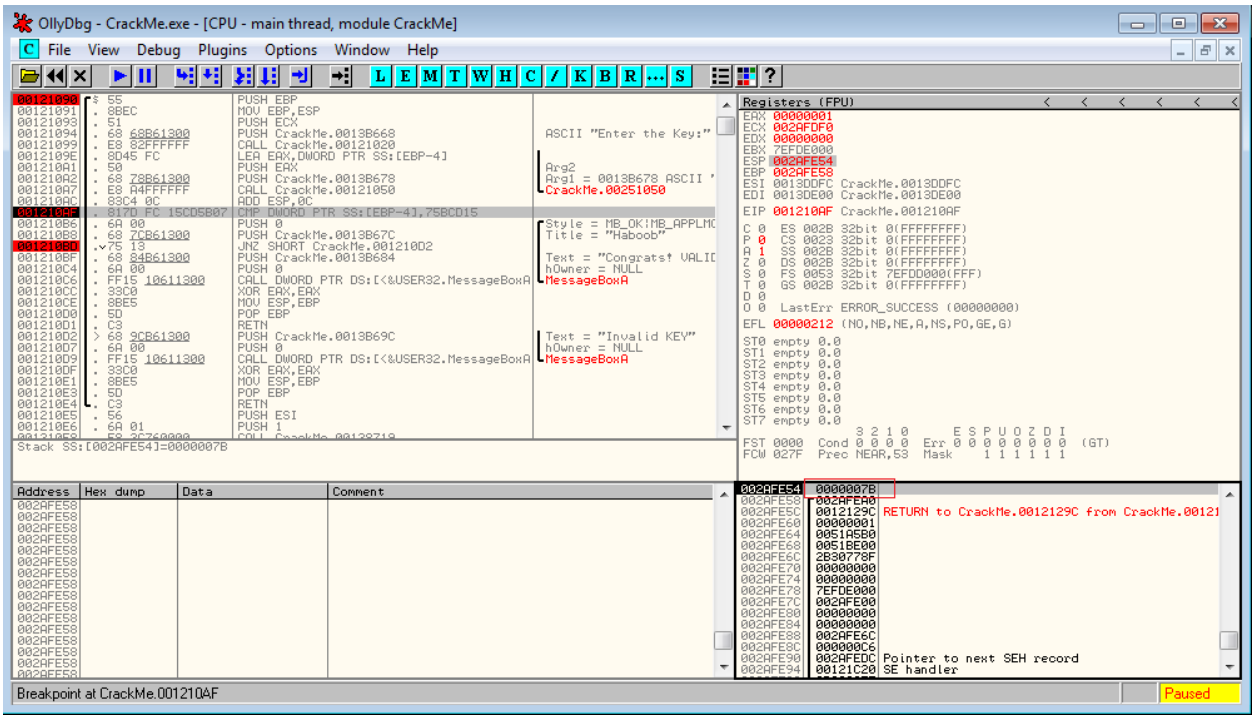
نلاحظ انه اذا تم تحويل القيمة 75BCD15 (والتي تم مقارنتها في القيمة الموجوده في الـ [EBP-4]) من النظام الست عشري (hexadecimal) الى النظام العشري (decimal) نحصل على هذه القيمة "123456789" كما في الصورة ادناه.



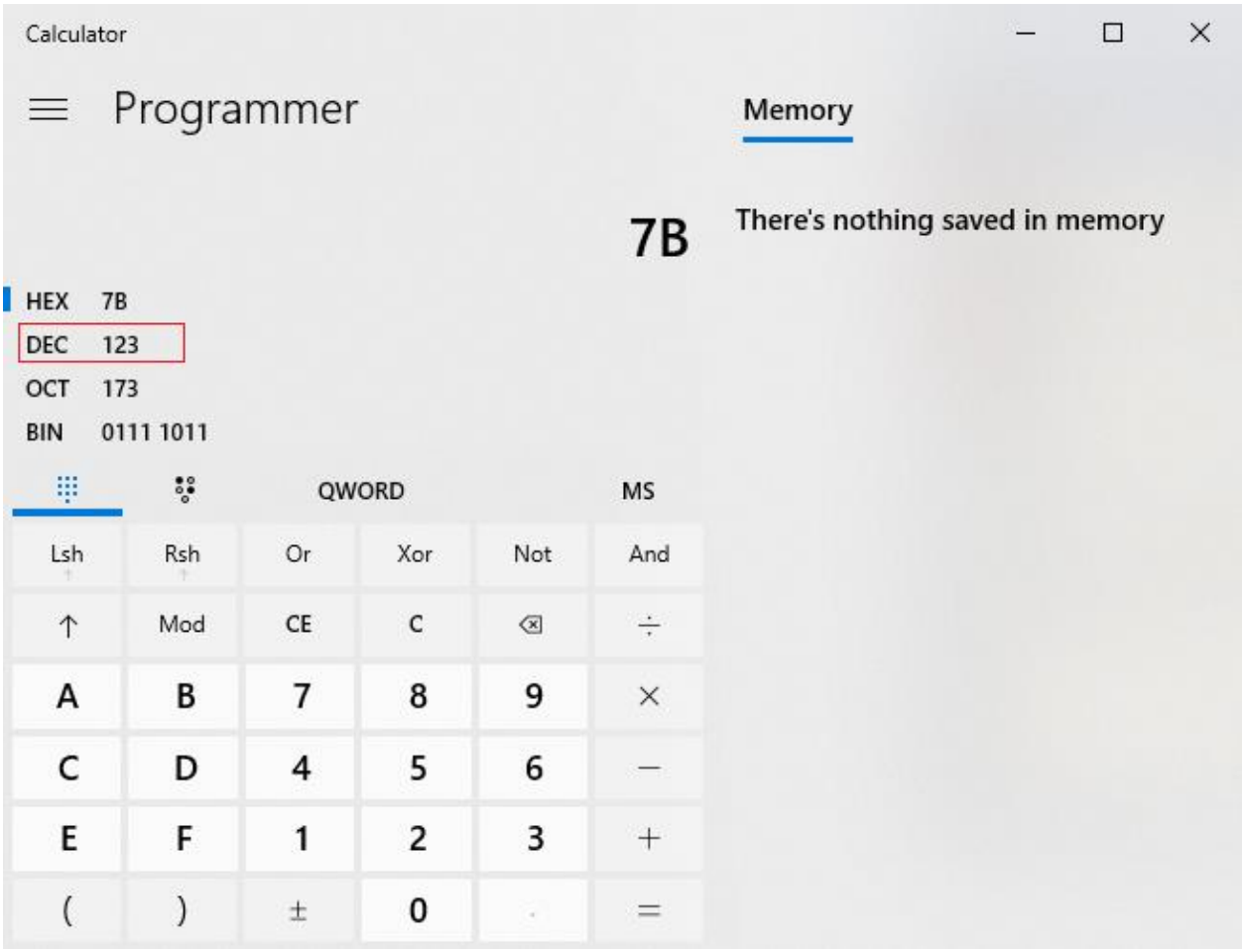
لنرى الآن ماهي القيمة الموجوده بداخل هذا المسجّل "Register" عن طريق تتبّع الصور:



قمنا بالضغط على مسجّل الـ ESP موجّة الستاك "Stack Pointer" المحدد بالمربع الأحمر الأول ومن ثم الضغط على الزر الأيمن في الفاره واختيار "Follow in Stack" في المربع الأحمر الثاني.



لنحصل على هذه القيمة الموضحة بالصورة اعلاه بالمربع الأحمر.



وعند تحويل القيمة الموجودة في مسجّل الـ EBP من النظام الست عشري (hexadecimal) الى النظام العشري (decimal) نحصل على القيمة في الصورة اعلاه ولايلزم وجود الأصفار.

نلخص ذلك بانه في العملية الثانية عند العنوان 001210AF. يتم مقارنة الرقم "123456789" بالرقم المدخل سابقاً "123" مايعني:

في العملية الثانية, عند العنوان 001010AF يتم مقارنه الرقم "123" بالرقم "123456789"

في العملية الثالثة, عند العنوان 001210BD :

- اذا كانت القيمة 123 لاتساوي 123456789 سيتم الانتقال الى عنوان الذاكرة (001010D2) وهي رسالة الخطأ.
- اما اذا كانت القيمة المدخلة 123 تساوي 123456789 لن يتم الانتقال الى عنوان الذاكرة (001010D2)(رسالة الخطأ) وسيتم تنفيذ العملية التي تليها في هذا العنوان 001010BF مما سوف يعطينا رسالة ان رقم السريال نمر صحيح.

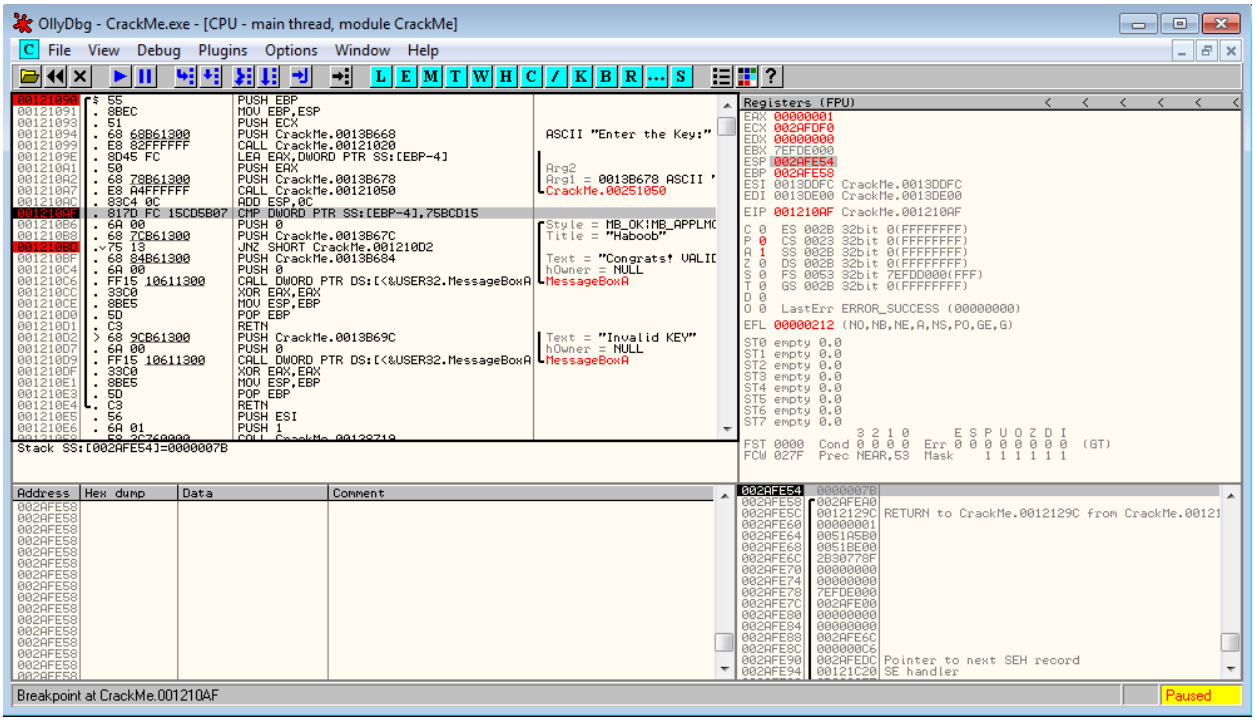
ونكون بذلك حصلنا على الرقم السري او السريال نمبر الخاص بالبرنامج.

في الطريقة الثانية سيتم التلاعب بالعمليات او الأوامر والتعديل عليها ليقبل البرنامج أي رقم سري نقوم بإدخالة. ومايهمنا هنا هي العملية الثالثة, عند العنوان 001210BD عملية الإنتقال المشروط "JNZ SHORT CrackMe.001210D2"

في برنامج الـ Olly والبرامج الأخرى المشابهة يمكننا التعديل على العمليات ويوجد اكثر من طريقة لجعل البرنامج يقبل أي رقم سري مدخل.

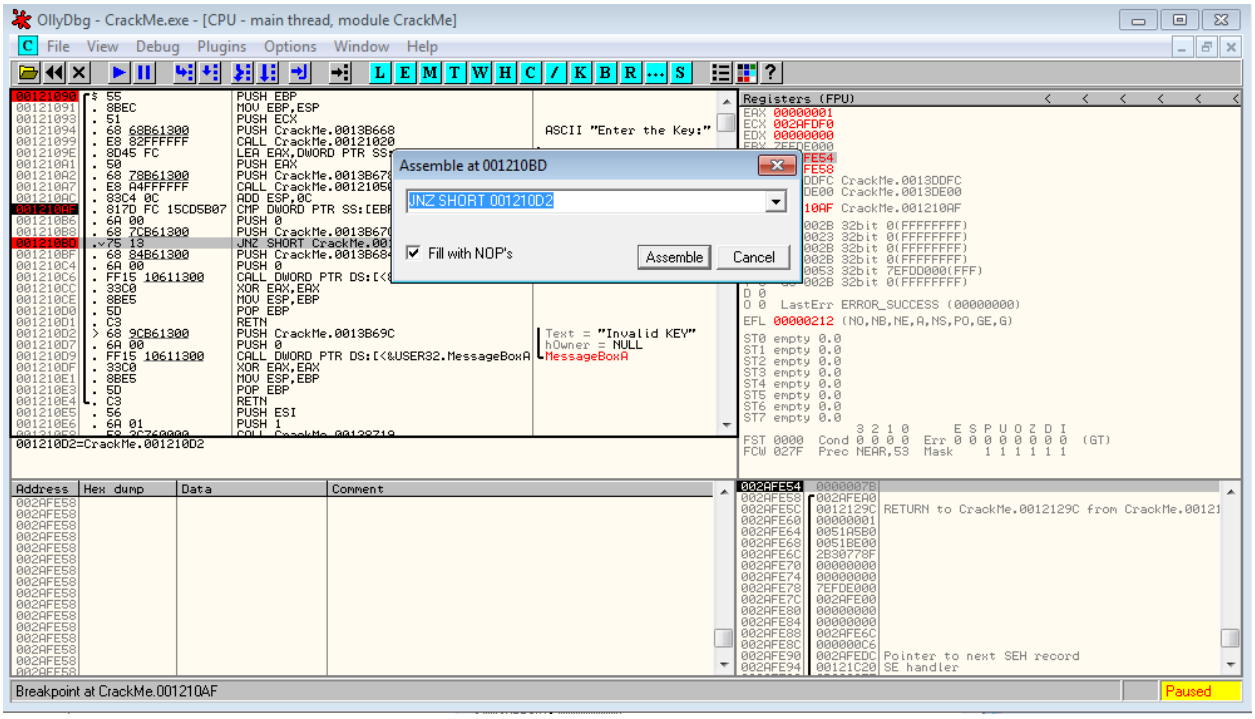
الطريقة الأولى يتم تعديل عملية الإنتقال المشروط "JNZ" لـ تصبح "JZ" وتعني ببساطة عكس الشرط اي انه اذا كان الرقم المدخل خاطئ سيتم إضهار الرسالة الصحيحه وهي ان الرقم السري المدخل صحيح, والطريقه الثاني مسح العملية بالكامل واضافة عملية او أمر الـ "NOP" "No Operation" وتعني لايوجد عملية وسيتم تنفيذ العملية التي تليها ومن ثم حفظ التعديلات على البرنامج وحفظة من جديد.

بما اننا وضعنا ثلاثة نقاط كسر ومن ثم بدئنا بتشغيل البرنامج عند وصول برنامج الـ Olly الى العنوان 001210AF وهي نقطة الكسر الثانية كما في الصورة التالية

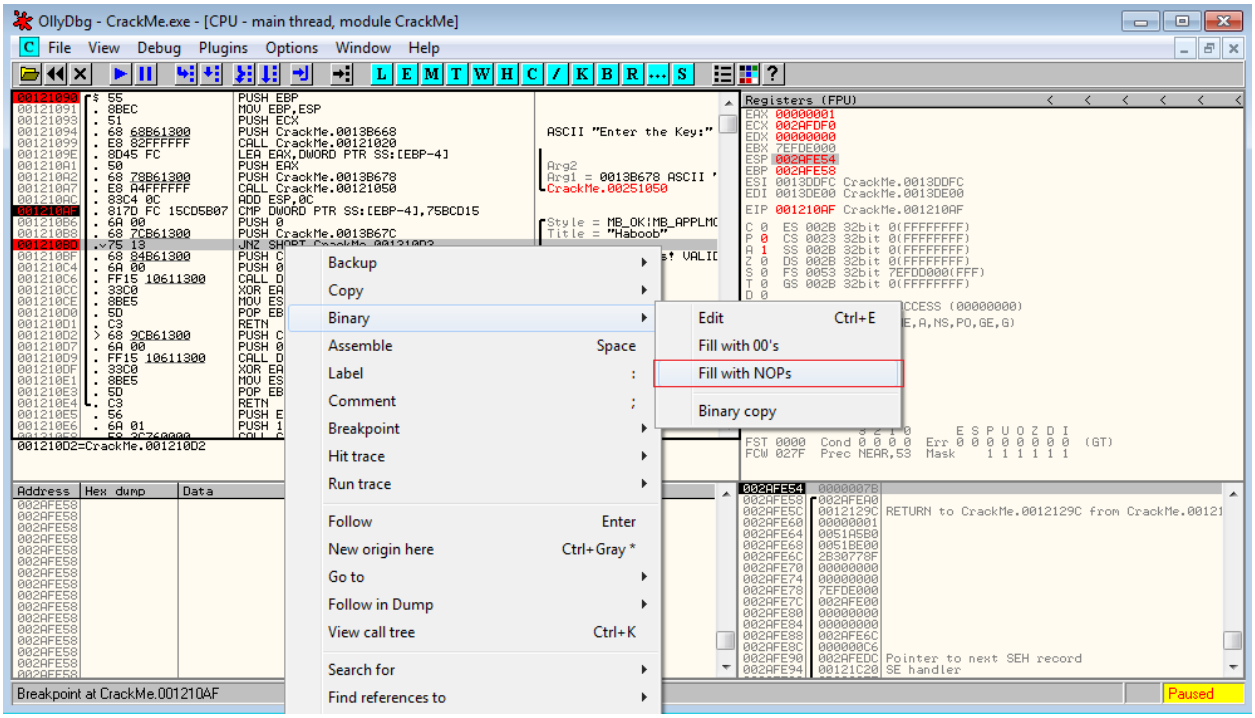


نقوم بعد ذلك بضغط زر الفاره مرتين على الامر المكتوب بجانب نقطة الكسر الثالثة عند العنوان 001210BD والذي يبدأ بـ"JNZ"

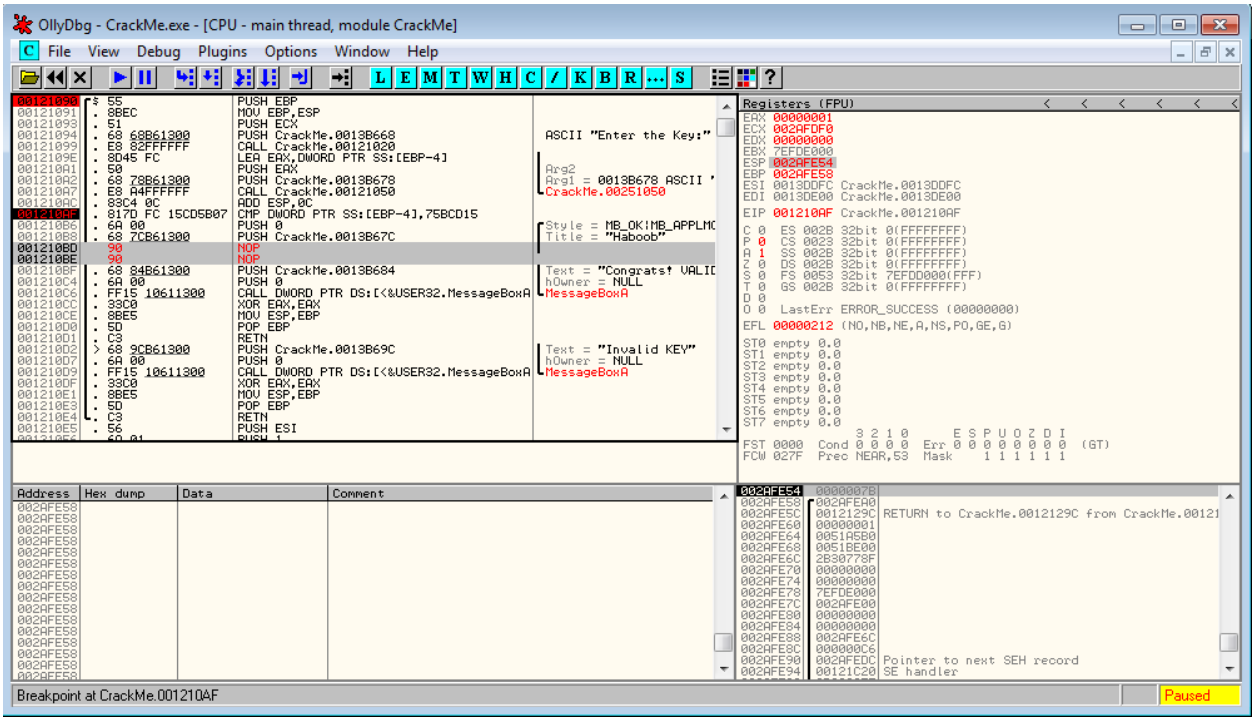
لتظهر هذه النافذة



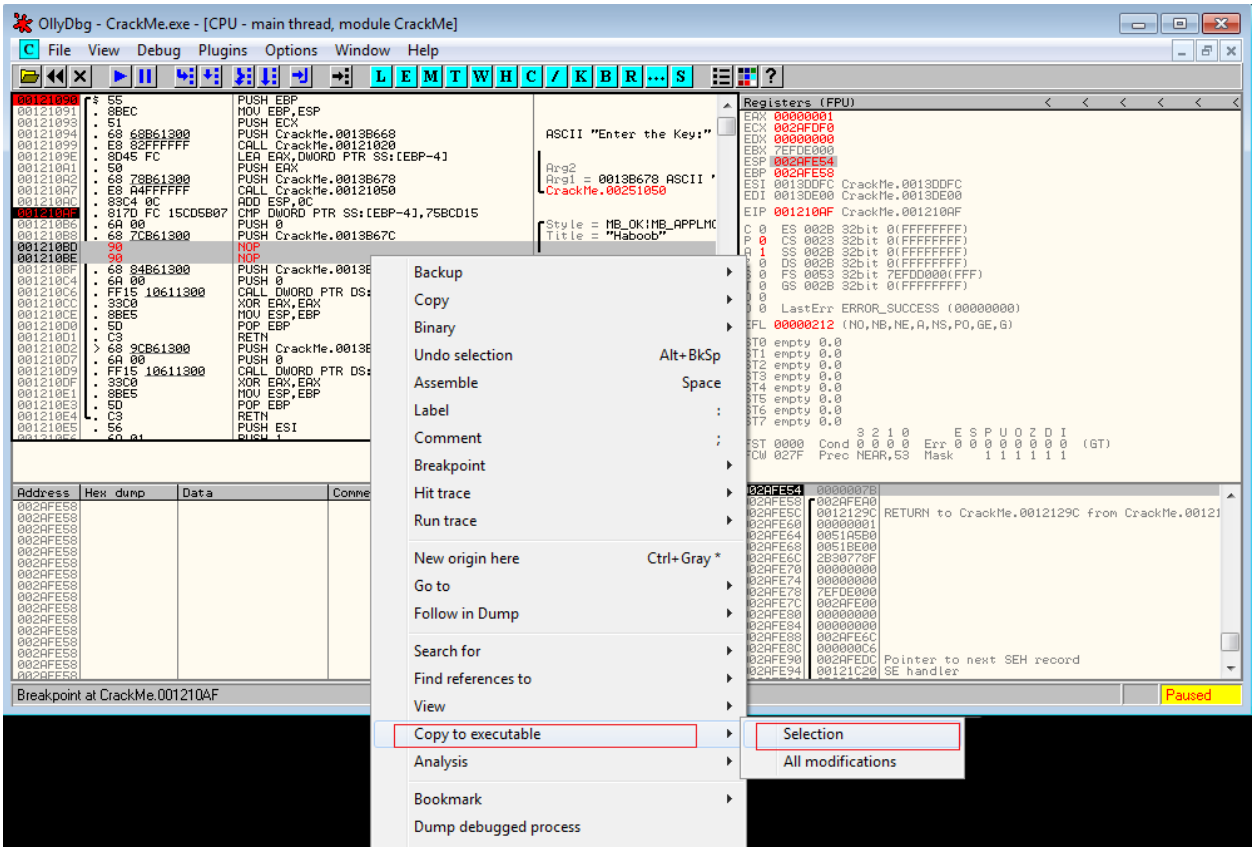
نقوم بعد ذلك بمسح حرف الـ N من الكلمة الأولى ليصبح الأمر "JZ" بدلاً من "JNZ" وتسمى هذه الطريقة التعديل المنطقي "Logic Editing" ويتم بعد ذلك حفظ التعديلات على البرنامج او بإستخدام الطريقة الثانية وهي الضغط بزر الفارة الايمن على العملية ومن ثم أختيار Binary ثم Fill with NOPs كما في الصورة التالية



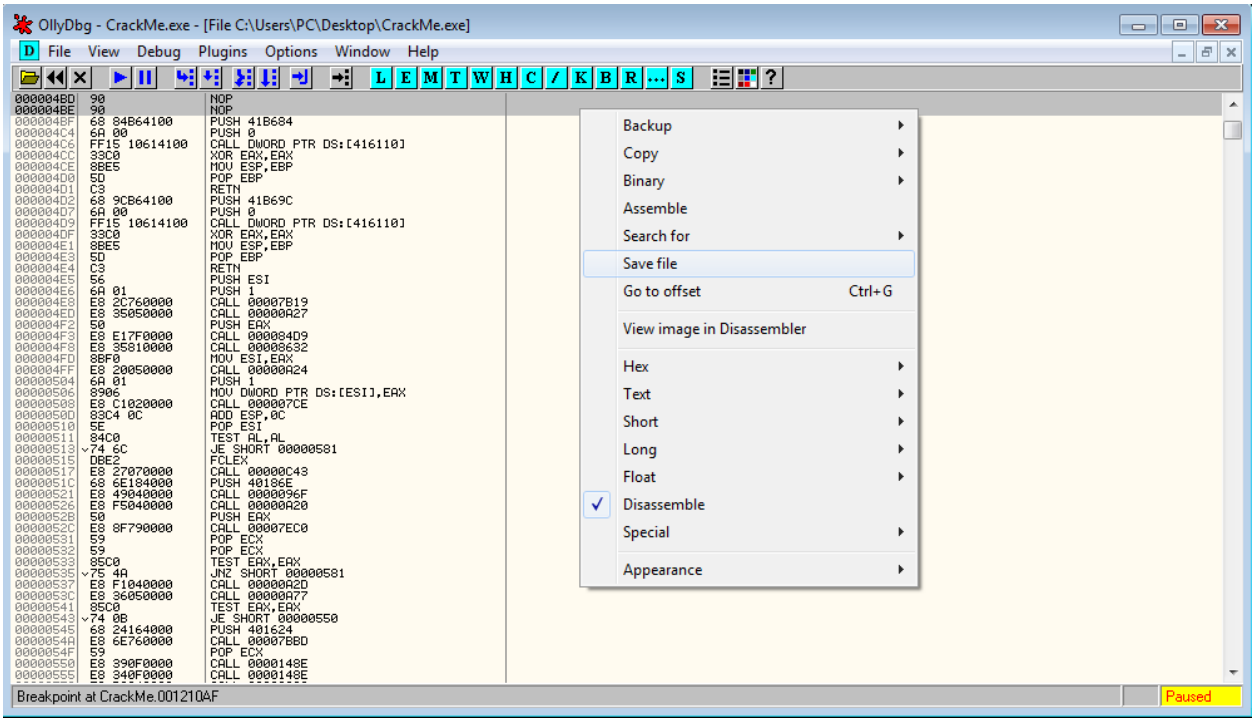
لتظهر الصورة النهائية هكذا:



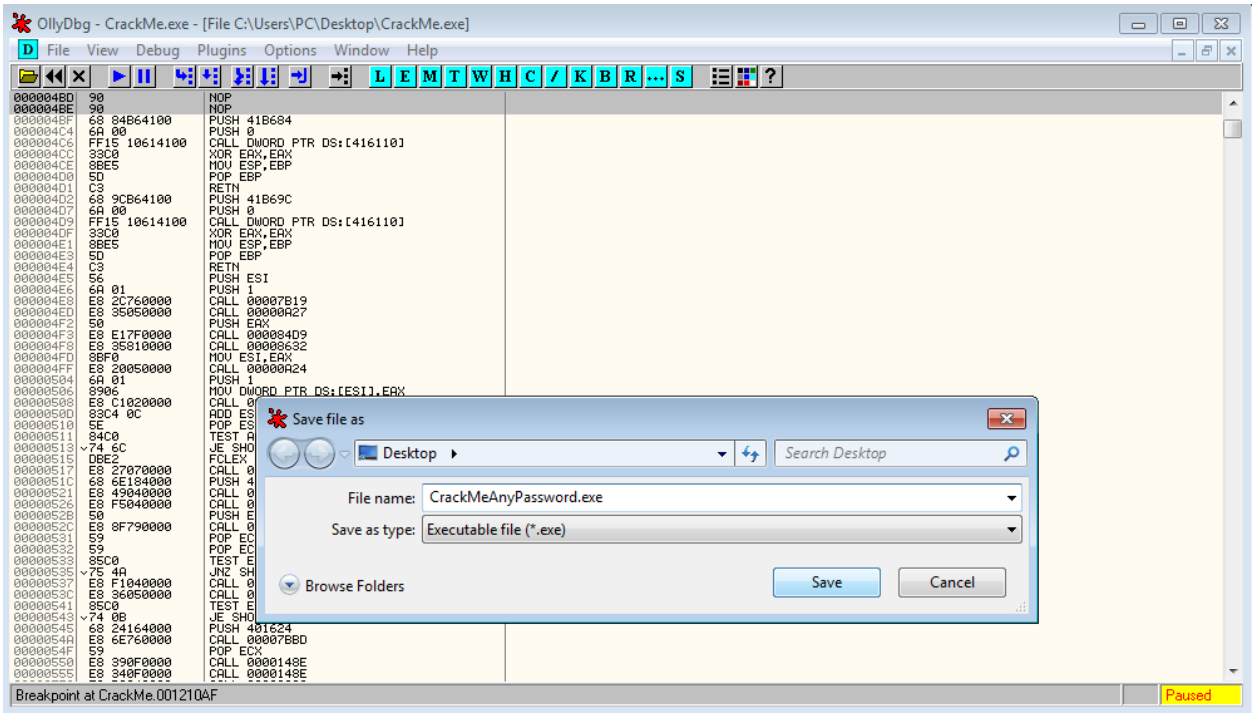
تم الانتهاء من التعديل و نلاحظ ان التعديلات على العملية اصبحت باللون الاحمر نقوم الآن بحفظ التعديلات على البرنامج بإتباع الصورة التالية.



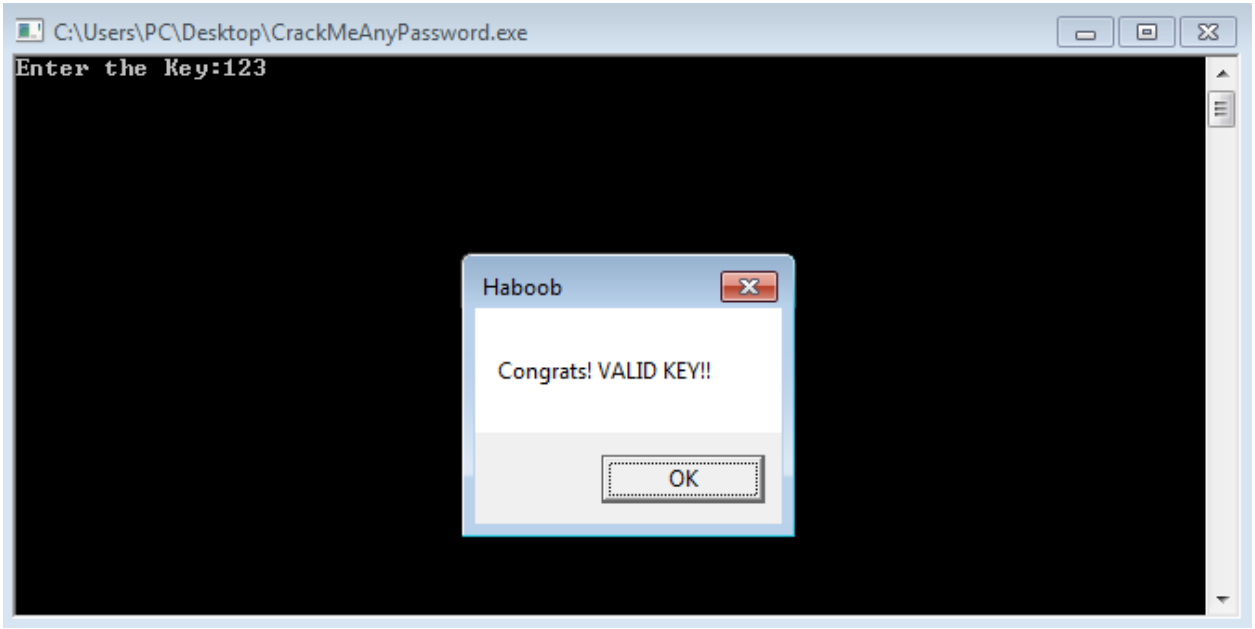
بعد الضغط على الخيار سيتم فتح نافذة جديدة نقوم بالضغط على الزر الايمن واختيار Save file



نقوم بإختيار الأسم الجديد للبرنامج ويتم حفظه.



الآن عند تشغيل البرنامج الذي قمنا بحفظة وادخال اي رقم سري تضهر لنا الرسالة الصحيحة كما في الصورة التالية:



إلى هنا ينتهي هذا الدرس.