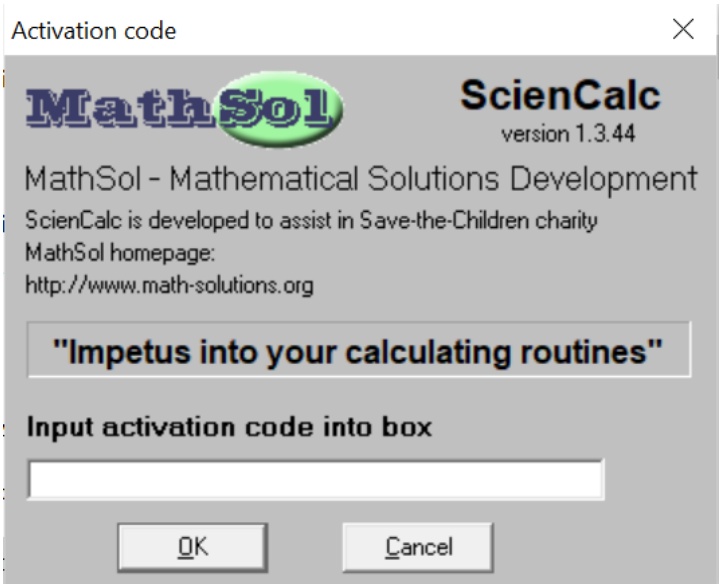
Bad license code @ http://www.math-solutions.org

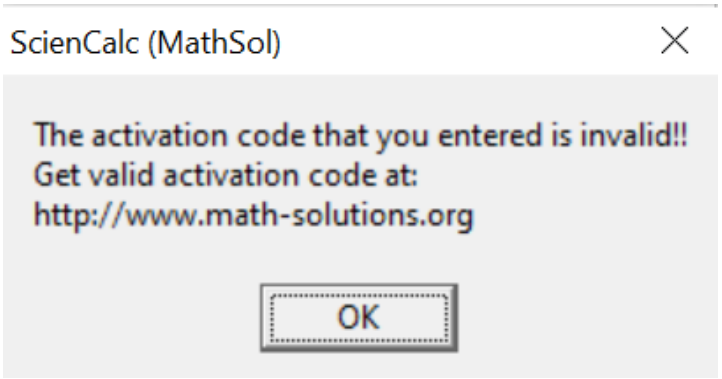
Despite: “All sales from MathSol applications are donated to the Children's Hospital.”
Payment for applications in MathSol (price: US$15 dollars per license)

- Nonlinear Regression - **CurveFitter**
- Equation Plotter - **EqPlot**
- Desktop Calculator - **DesktopCalc**
- Scientific Calculator - **ScienCalc**
- Multivariable Calculator - **SimplexCalc**
- Multipurpose Calculator - **MultiplexCalc**
- Compact Calculator - **CompactCalc**
- Nonlinear Analysis- **DataFitting**
- Innovative Calculator - **InnoCalculator**
- Unit Conversion - **UnitConvertor**-A .. D

When you first open a program you are prompted with this:



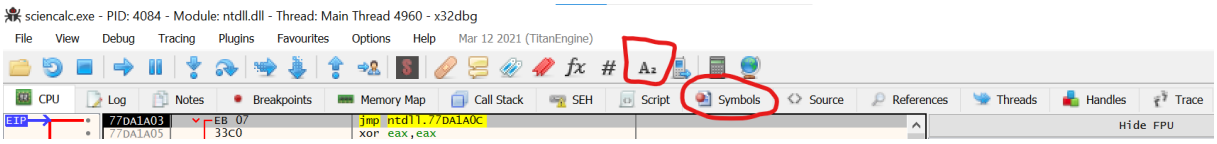
A dummy code gives us this:



We can use whatever debugger is handy. I use X32/64 DBG. The 32-bit is used here.

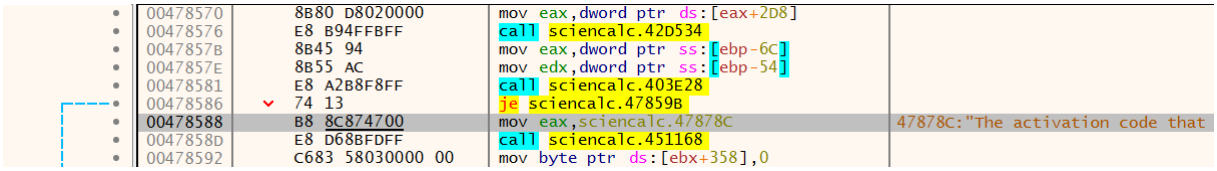
Open it up and load the program you want to check out. I use the ScienCalc.

Remember the ErrorMsg? Use X32DBG to search for that string:
First click on Symbols and doubleclick on our program. Usually at the top. Then click the Az button.

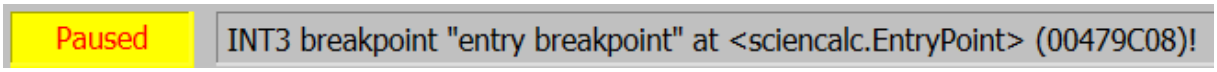


You can now search the strings:

Doubleclick that row and you will end up here:

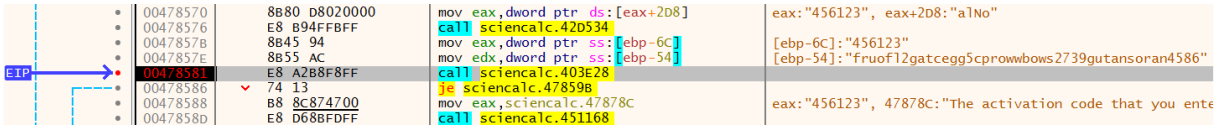


Now, the JE instruction one line above is a Jump If Equal. Equal to what? And do you see the blue line to the left? That where it takes us. But we didn't take that call, because we are just below. So what are compared? Let's find out by setting a BREAKPOINT at the CALL at address 00478581. Do so by doubleclick at the second column there, where it sais E8 A2B8F8FF. A red marker appears. Good.
Now click on Run. The icon looks like a right arrow. The 4th icon.
Look at the bottom of X32DBG:

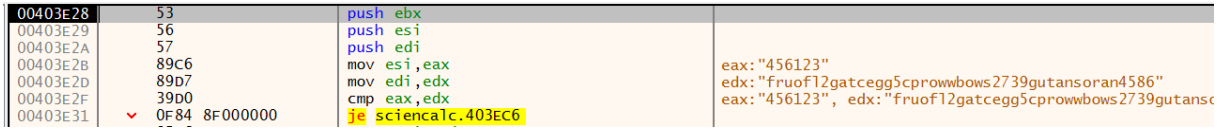


Two more times to:

Now the program is running and we can enter some dummy code in the box. Do so. I did "456123"



Scroll up a bit to see a bit more. Now that string above our CALL looks very suspicious… I wonder…
But go into the CALL now by pressing F7 or the 6th icon. A down arrow with a dot.



Ok, so this is fairly easy to understand. And very, VERY bad.
The PUSH is just a way to prepare the address. But the MOV is copying the value of EAX to ESI.
Then the CMP compares the two values. So, there you have it!

When you enter this code in the box, you won't get any confirmation. But if you run the program again, it won't show up. Good. The program is registered. Now for some detective work.

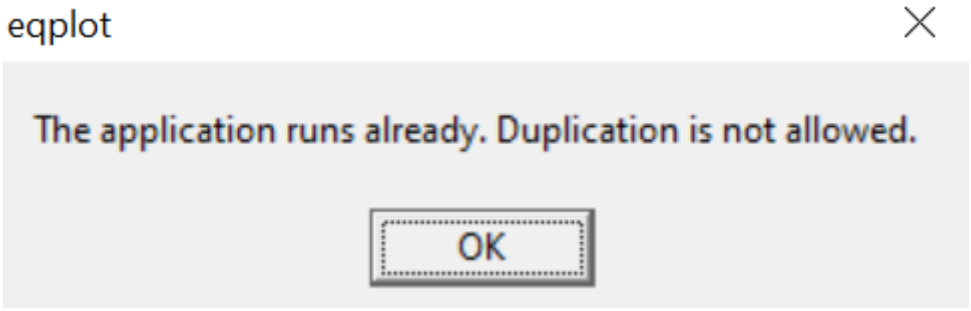
Where did it store this code? In a file? In the Registry? Well, we can manually check it.
Try looking in the directory where it is installed. Nothing. The INI file doesn't have it.
Ok, we can look in your User directory. But no luck here either.
So, next step might be the registry. Open REGEDIT and search. Just the regcode can't be found but we could have traced the app a bit more in X32DBG to find some more strings.

```
0019F81C | 022E93B4 | "456123"
0019F820 | 022E544C | "63E07CD666F952FC5AEE4FED59FE"
0019F824 | 022EA100 | "1376616515"
0019F828 | 022EA0D4 | "69EE4AE470C38DB784D06DC38CC9"
0019F82C | 022EB000 | "MathSol Development\\Activation code\\Designations\\Ly
0019F830 | 022EA450 | "fruofl2gatcegg5cprowwbows2739gutansoran4586"
```

That 0019F82C looks promising. Let's check that out.
Yes! Here it is. But it's not our code there is something else. Note that down. Export this RegKey.

Let's download another app from that site. Run it. Hmm, unregged. Ok, repeat the process.
Same input code! Wow.. Too easy. Again, notice the RegKey. Here IS a difference! Cool!

Also if we try to run another app while the first one is running, we get an error. That is because the license key are stored in the same place, but use a different key.



So we need to manually input that code everytime we switch apps.
I will write down all RegKeys here now:

CurveFitter = 66E37FD361F25DE775C393A9A2A7
EqPlot = 69EE4AE470C38DB784D06DC38CC9
DesktopCalc = 67EC481A3B143C0653E17CD07ADF
ScienCalc = 63E07CD666F952FC5AEE4FED59FE
SimplexCalc = 62E773CF6DC68EB08DDB7AD670D5 (under \Sysrq)
MultiplexCalc = 6AEF4BE775CE79DB79CF6EC28DCA
CompactCalc = 64E17DD163FC57F9471D39173015
DataFitting = 65E27ED06CC781C390A4B28EB99E
InnoCalculator = 68ED49E577C880C29FB581DF6BE8
UnitConvertorA = 51F6421C390A420C293F1F3D1633 no…?
UnitConvertorB = 52F7431F3E113B0552E677D571D6 no…?
UnitConvertorC = 53F04CE676C983CD6BF944183310 no…?
UnitConvertorD = 54F14DE173CC84CE6CF8451B3411 no…?

Dator\HKEY_CURRENT_USER\SOFTWARE\MathSol Development\Activation code\Designations\Ly110227x\Secure

fruofl2gatcegg5cprowwbows2739gutansoran4586

[HKEY_CURRENT_USER\SOFTWARE\MathSol Development\Activation code\Designations\Ly110227x\Secure]