## Static Analysis

Using x64dbg

## Static Analysis vs Dynamic Analysis

- Static means not running the program
- Dynamic means running the program
- Using x64dbg we can do both:
  - run the program and examine memory and registers
  - examine the graphical view to gain better clarity

## Why Static Analysis?

We can get a graphical view of the program

```
00401000 <crackme4.sub 401000>
                                                push ebp
                                                mov ebp,esp
                                                sub esp,10
                                                push 0
                                                push <crackme4.sub_4010F0>
                                                push 0
                                                push 81
                                                push dword ptr ss:[ebp+8]
call dword ptr ds:[<&CreateDialogParamA>]
                                                push 1
                                                push eax
                                                mov dword ptr ds:[4142A4],eax
                                                 call dword ptr ds:[<&ShowWindow>]
                                                push crackme4.4142E8
                                                 call dword ptr ds:[<&GetLocalTime>]
                                                movzx eax, word ptr ds:[4142EE]
                                                mov ecx,1E; ecx:EntryPoint
                                                sub ecx, eax; ecx: EntryPoint
                                                mov dword ptr ds:[4142A0],ecx; ecx:EntryPoint
                                                test ecx,ecx; ecx:EntryPoint
                                                 ig crackme4.401055
crackme4.00401055
                                                                              crackme4.0040104E
                                                                               push crackme4.411AE8 ; 411AE8:"Trial Period has expired"
push ecx ; ecx:EntryPoint
push crackme4.411B04; 411B04:"%d days trial period remaining\n"
                                                                                imp crackme4.40106E
push crackme4.4142A8
call dword ptr ds:[<&wsprintfA>]
add esp,C
push crackme4.4142A8
```

## Thank you