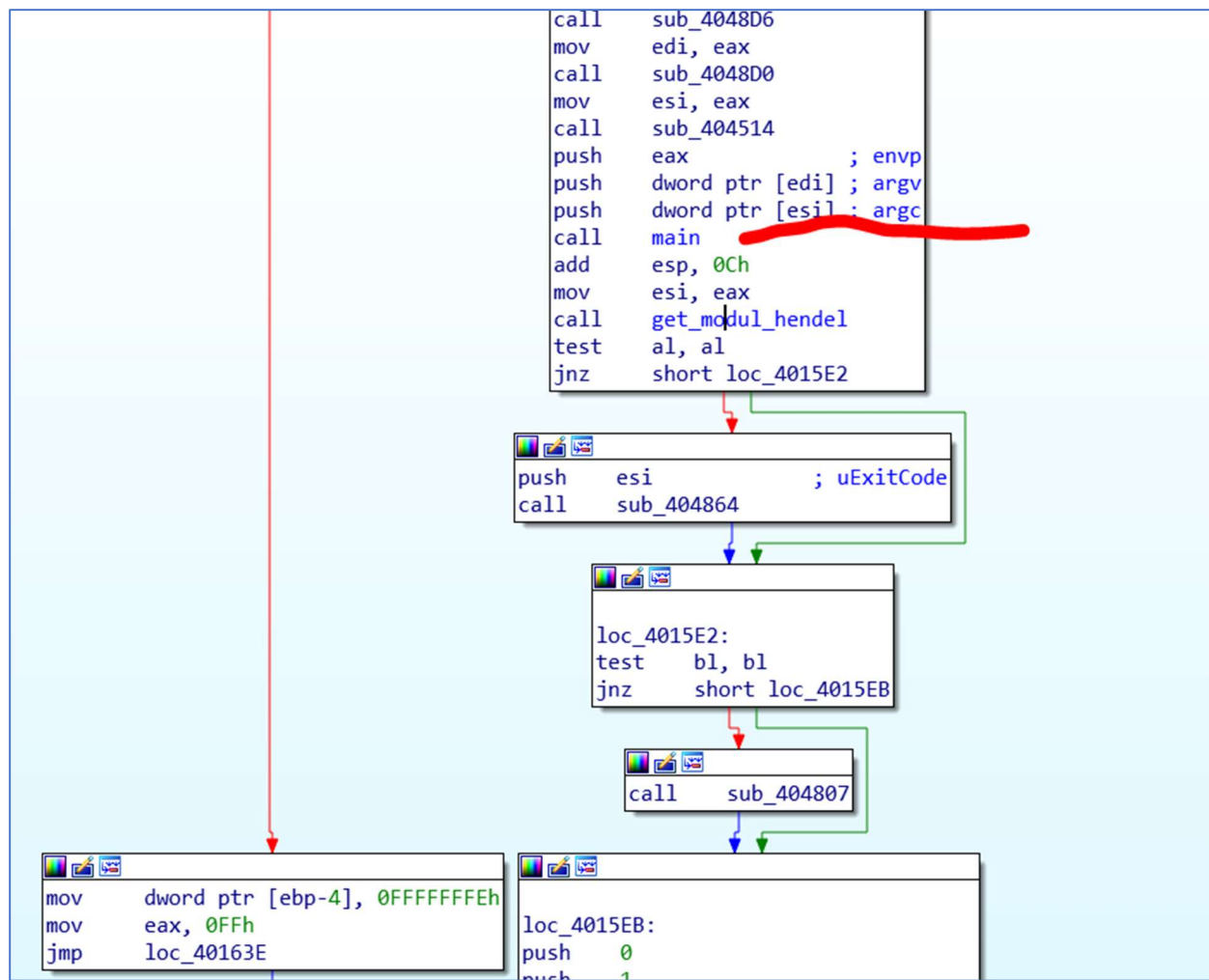


בהתחלה נמצא איפה מתחיל ה:main



ניכנס ל:main

רואים שיש כמה פונקציות,

```

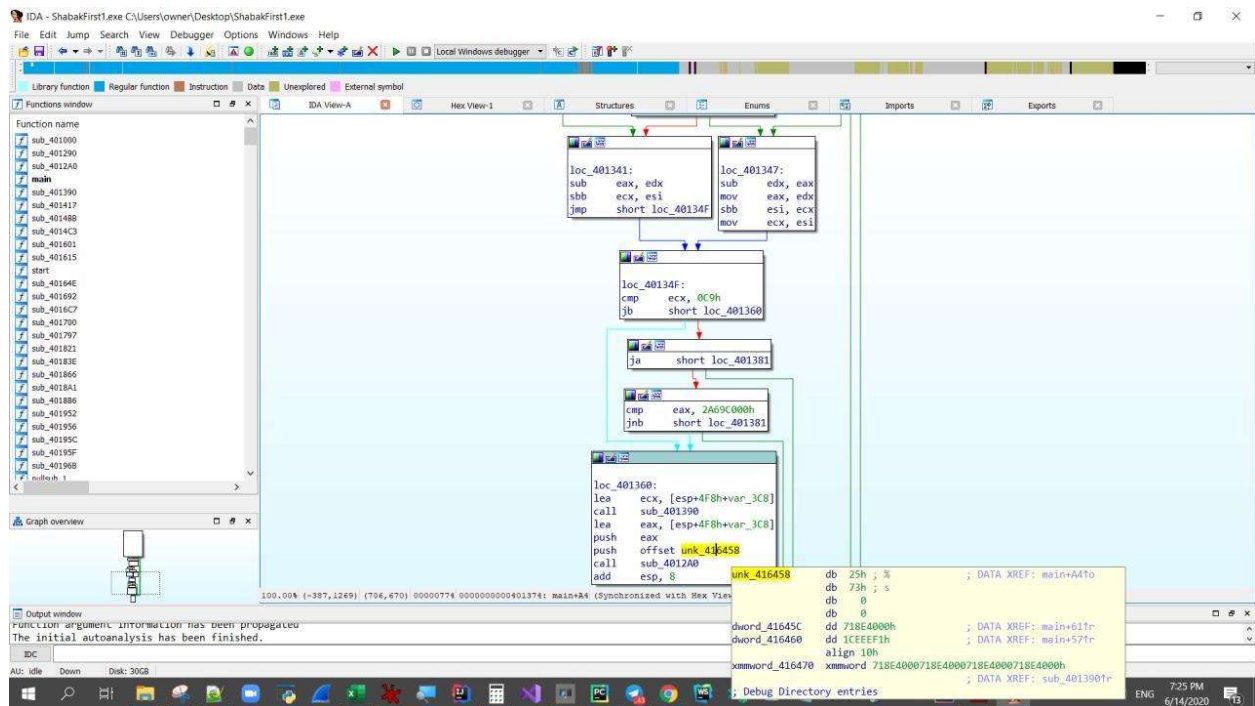
; int __cdecl main(int argc, const char **argv, const char **envp)
main proc near

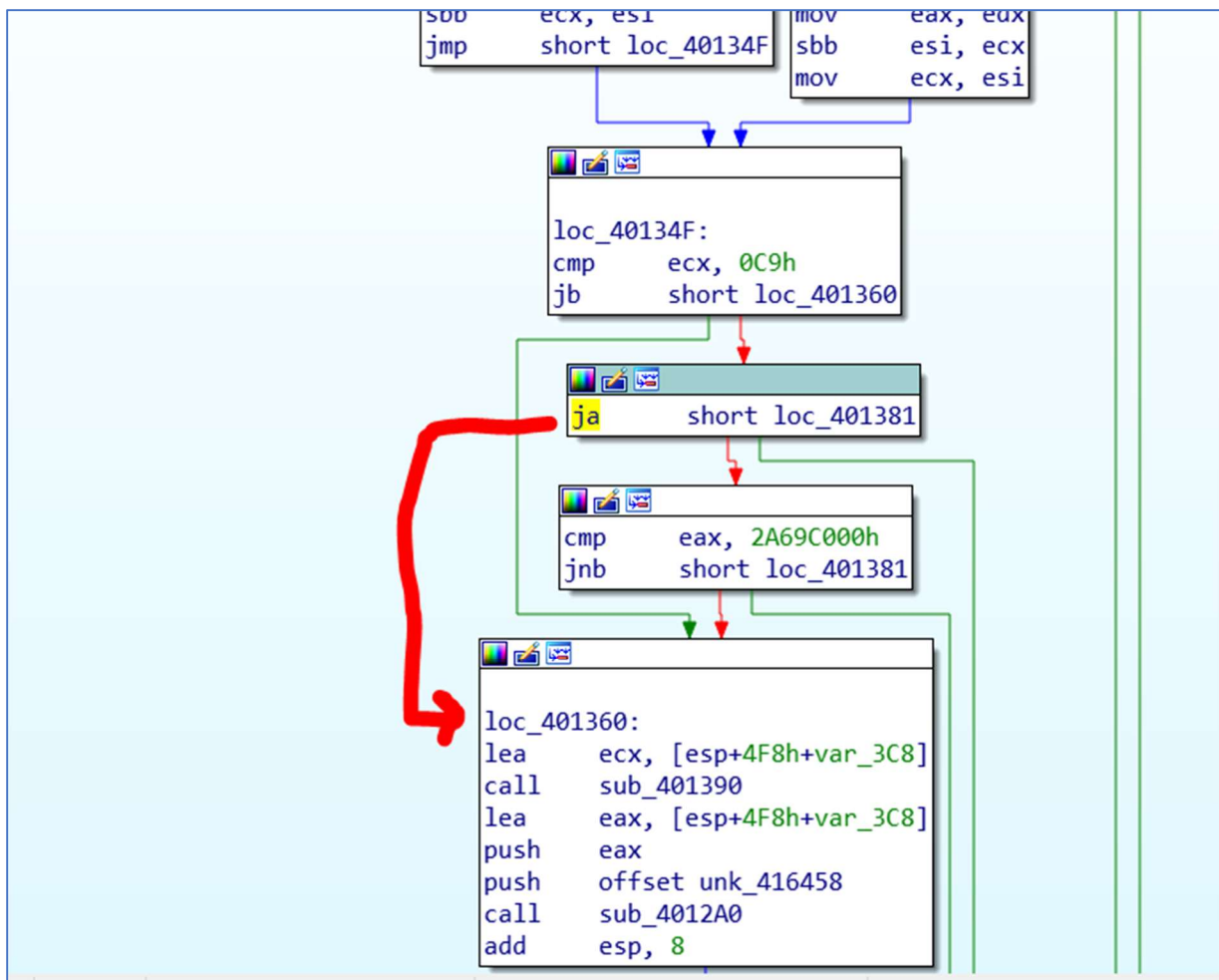
FileInformation= byte ptr -4F4h
var_4E8= dword ptr -4E8h
var_4E4= dword ptr -4E4h
Dst= byte ptr -4D0h
var_3C8= byte ptr -3C8h
argc= dword ptr 8
argv= dword ptr 0Ch
envp= dword ptr 10h

push    ebp
mov     ebp, esp
and     esp, 0FFFFFFFh
sub     esp, 4F4h
lea     eax, [esp+4F4h+Dst]
push    esi
push    104h
push    0
push    eax
call    const_variboles
add     esp, 0Ch
lea     eax, [esp+4F8h+Dst]
push    104h                ; nSize
push    eax                ; lpDst
push    offset Src         ; "%PROGRAMFILES%\messeeker inc"
call    ds:ExpandEnvironmentStringsA
lea     eax, [esp+4F8h+FileInformation]
push    eax                ; lpFileInformation
push    0                  ; fInfoLevelId
lea     eax, [esp+500h+Dst]
push    eax                ; lpFileName
call    ds:GetFileAttributesExA
test    eax, eax
jz      short loc_401381

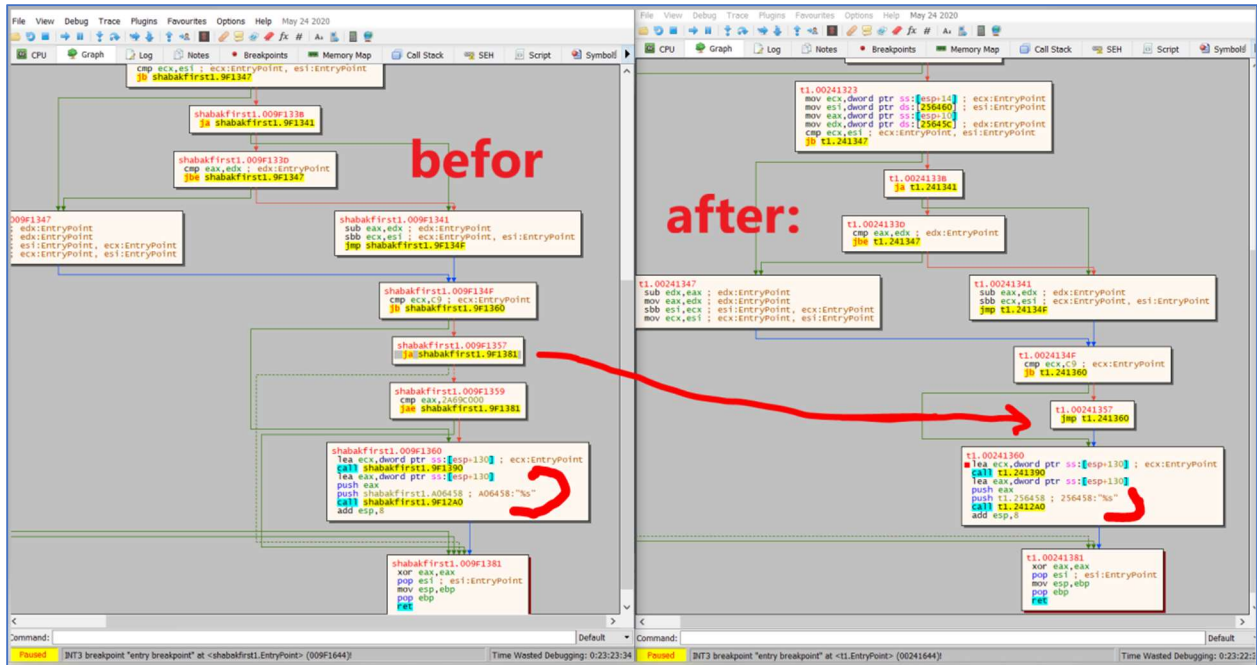
```

רואים שיש פונקציה שלשם שלוחים גם S%





כלומר אם מצליח להגיע לפונקציה הזו נוכל לגרום לו להדפיס  
 אבל כשעקבתי אחרי הפונקציה ראיתי שלא נכנס לפונקציה,  
 ולכן שיניתי במקום שידלג, כתבתי jmp  
 ככה נראה הקוד לפני ואחרי:



כשהגיע לפונקציה הוא אכן הדפיס למסך:

t1.exe - PID: 14F8 - Module: t1.exe - Thread: Main Thread 14BC - x32dbg

File View Debug Trace Plugins Favourites Options Help May 24 2020

CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads

Address	Disassembly	Comment
00241360	lea ecx, dword ptr ss:[esp+130]	
00241367	call t1.241390	
0024136C	lea eax, dword ptr ss:[esp+130]	
00241373	push eax	
00241374	push t1.256458	
00241379	call t1.2412A0	
0024137E	add esp, 8	
00241381	xor eax, eax	
00241385	pop esi	
0024138A	mov esp, ebp	
0024138E	pop ebp	
00241387	ret	
00241388	cc	
00241389	int3	
0024138A	cc	

256458: "%s"

C:\Users\owner\Desktop\t1.exe

```

*-----*
/
Great Job!
Your password is:
Never_Clean_DNA_Vials_With_Your_Spit
\
*-----*

```