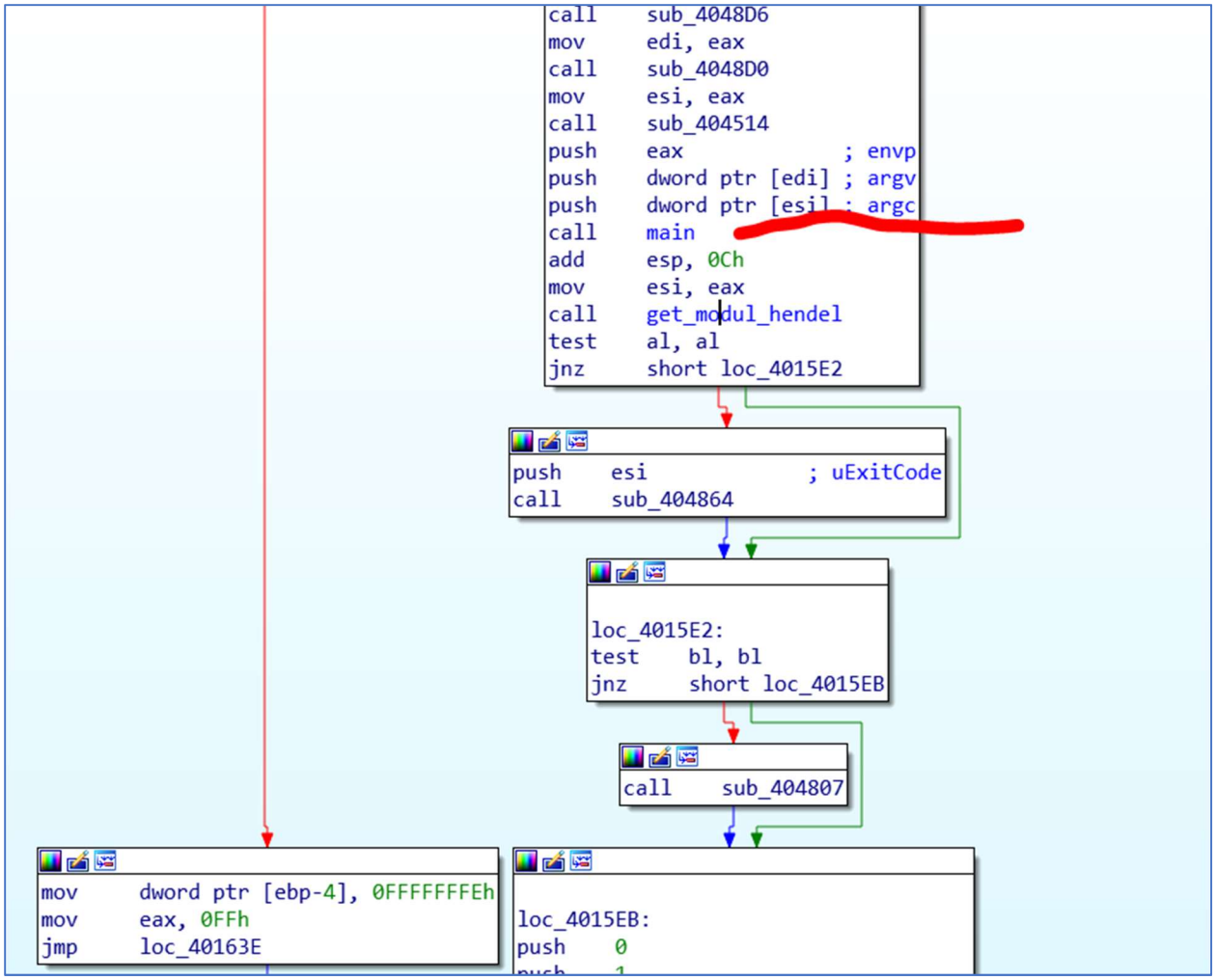
תרגיל ShabakFirst

בהתחלה נמצא איפה מתחיל ה:main



ניכנס ל:main

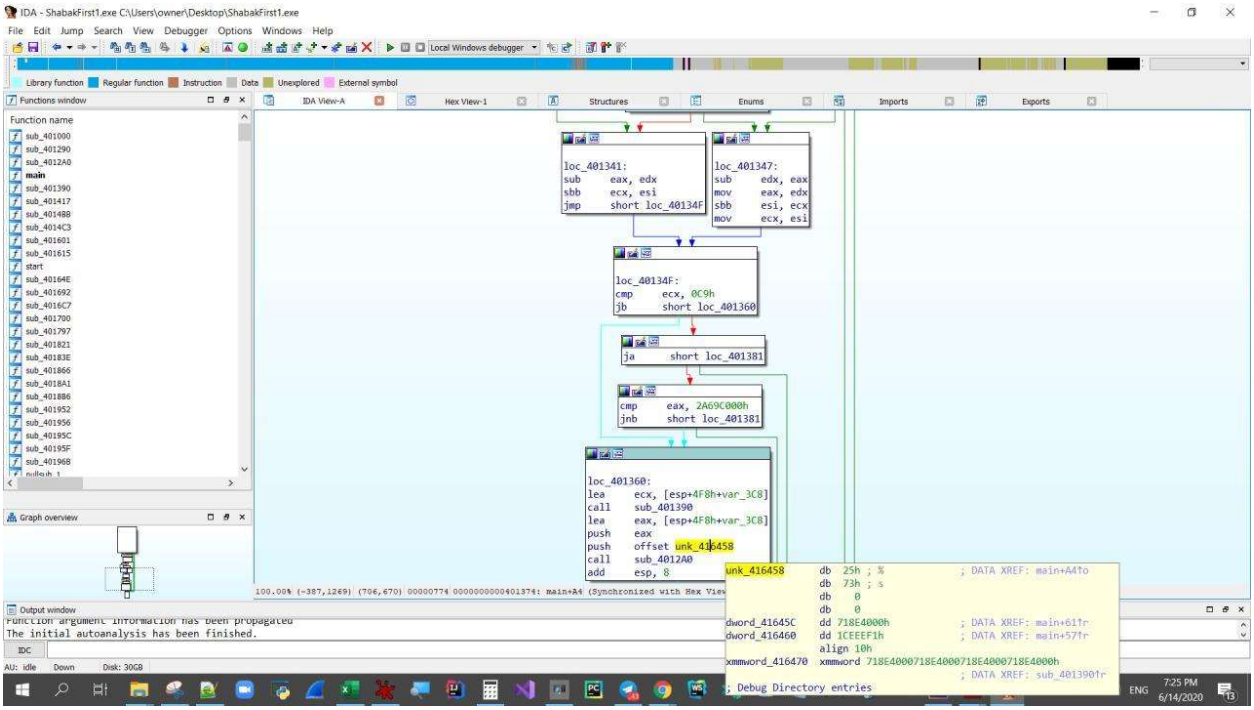
רואים שיש כמה פונקציות,

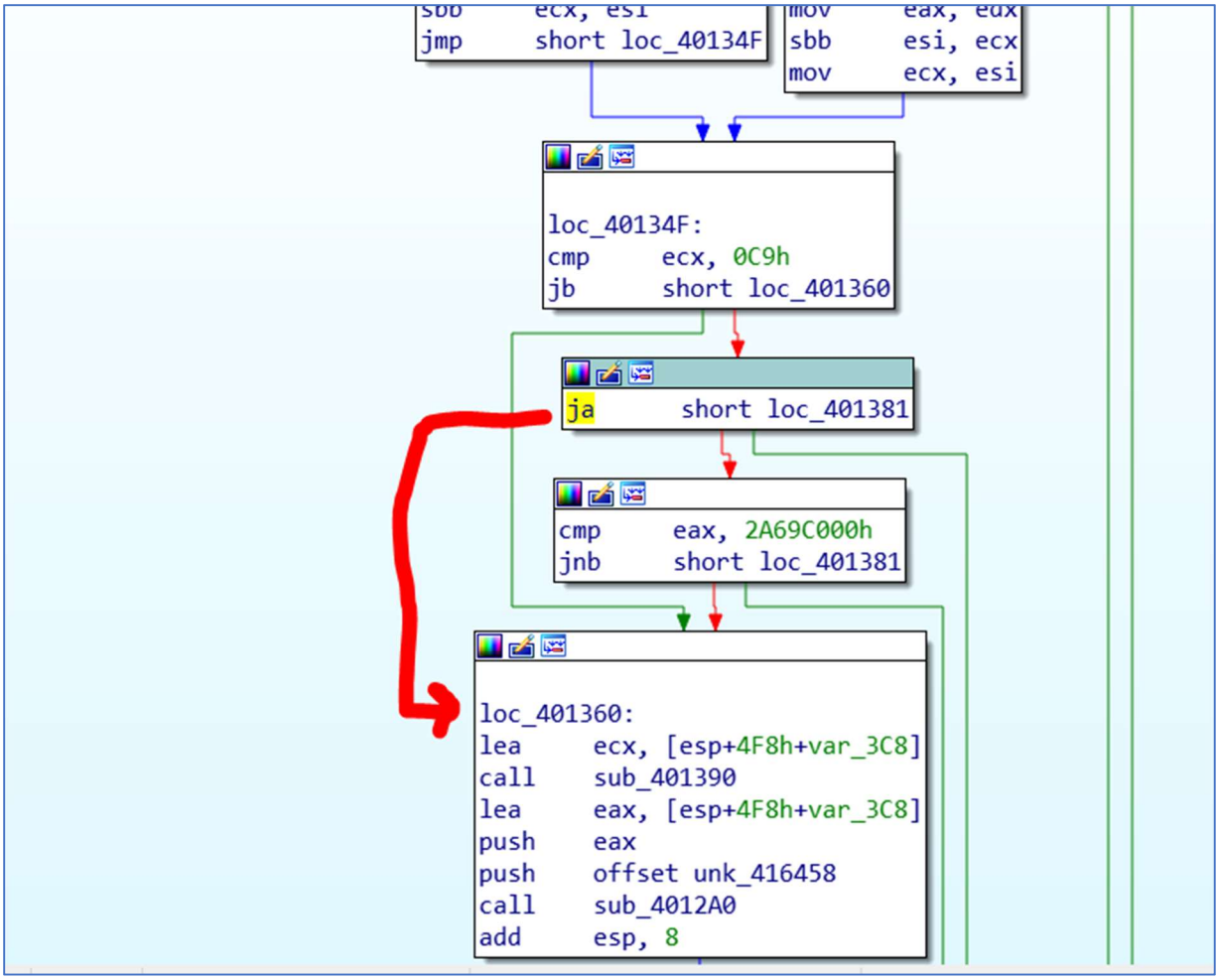
```
; int __cdecl main(int argc, const char **argv, const char **envp)
main proc near

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, 0FFFFFFF8h
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%\\meseeker 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



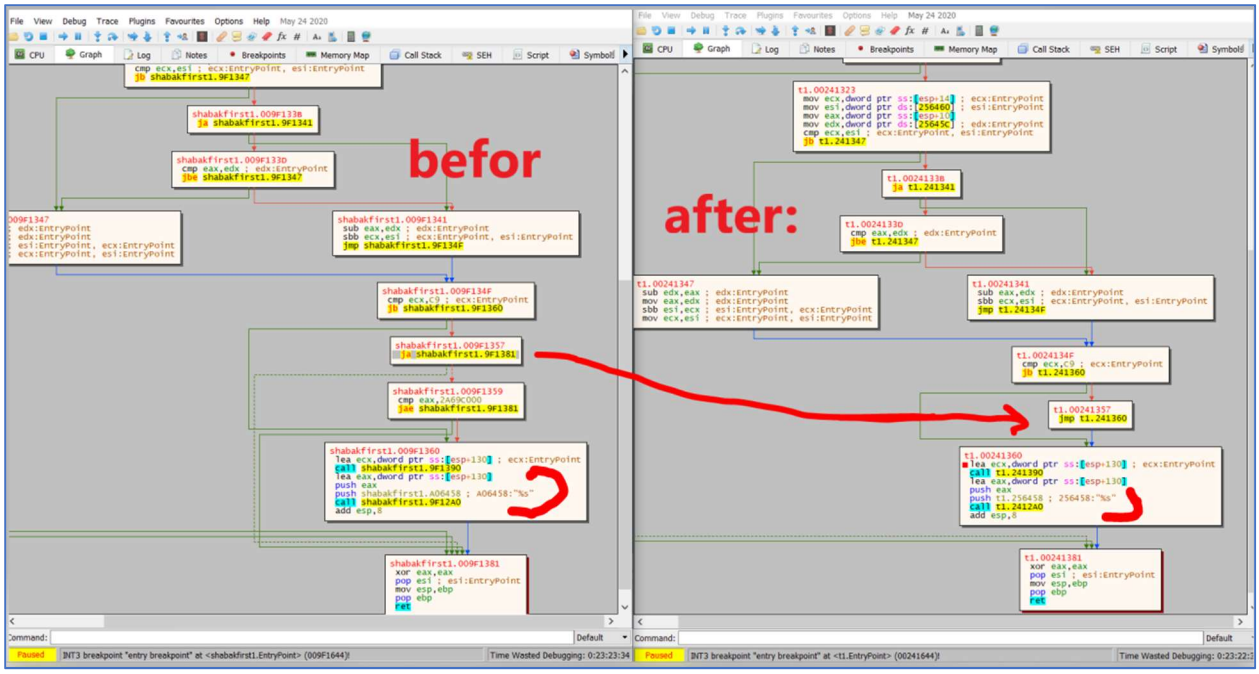


כלומר אם מצליח להגיע לפונקציה הזו נוכל לגרום לו להדפיס

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: