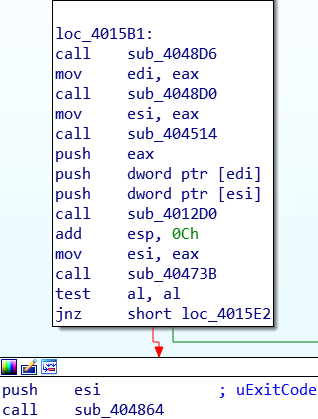
תרגיל בית שב"כ נועם כהן:

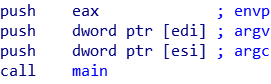
בשלב הראשון עלינו למצוא את פונקציית הmain.  
כמו שלמדנו, נרד כמה שיותר לסוף הקוד, והmain אמור להיות לפני הexitcode.  
כמו כן, בד"כ לפני הקריאה של הmain נראה במפורש push של 3 ערכים:



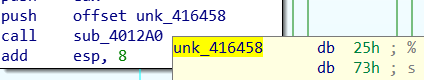
אנו רואים באלגוריתם הראשון לפני הקריאה ל sub\_4012D0 דחיפה של 3 ערכים. בנוסף, הפונקציה מופיע ממש קצת לפני הexitcode.  
ניכנס לפונקציה הנ"ל:



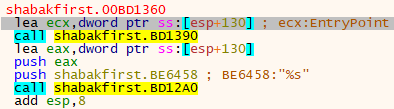
והגענו לmain. נשנה את שם הפונקציה לmain:



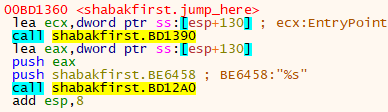
נרד קצת למטה:



כפי שאנו יכולים לראות, בפקודה push offset unk\_416458 אנו יכולים לראות %s- ז"א שמדובר במחרוזת.  
מטעמי נוחות, נעבור ל x32dbg, נגיע לmain, ונרד לאזור הקוד בו מופיע ה%s:



נשים בשורה הראשונה label ונקרא לו jump\_here. אנו עושים זאת כיוון שאנו מניחים שכאן מתבצעת ההדפסה של מה שאנחנו רוצים.



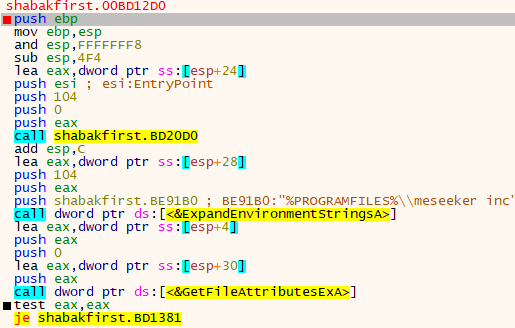
כעת ניגש לפקודה text eax, eax :



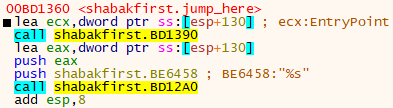
ונשנה אותה לפקודה jmp jump\_here:



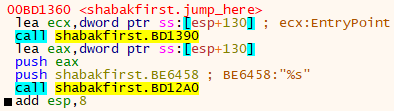
נשים breakpoint בתחילת ובסוף הקוד ונריץ:



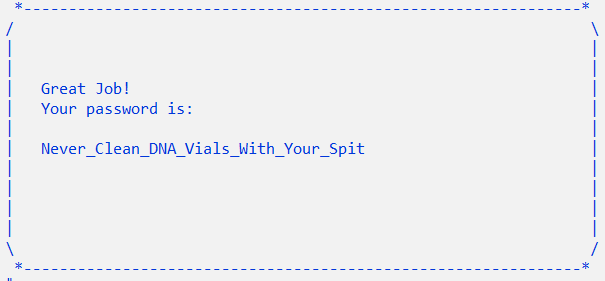
הגענו לפקודה test eax, eax (ששינינו אותה ועכשיו היא jmp jump\_here)  
עכשיו נמשיך ונראה שזה יקפוץ לlabel ששמנו:



נמשיך עד אחרי פקודת הcall האחרונה:



ויצאה לנו התשובה הבאה:



סיימנו את התרגיל 😊 !