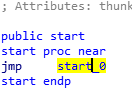
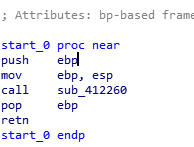
**מבחן מועד ב ברברסינג:**

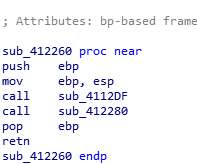
1. תחילה אנו צריכים למצוא את הmain בתוכנית. ניכנס לstart\_0:



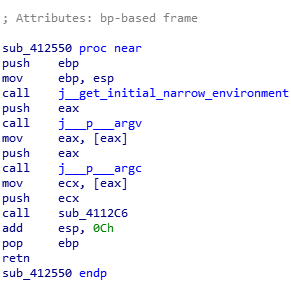
עכשיו לsub\_412260:



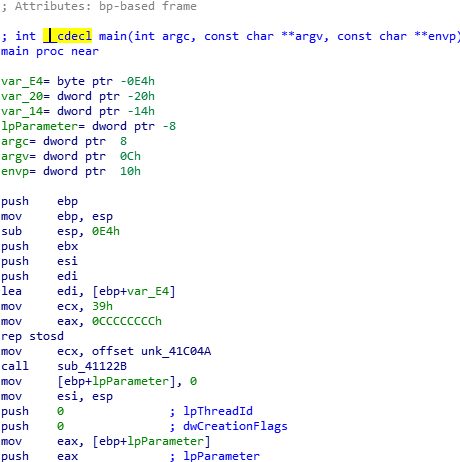
עכשיו לsub\_412280 (הפונקציה האחרונה כמובן):



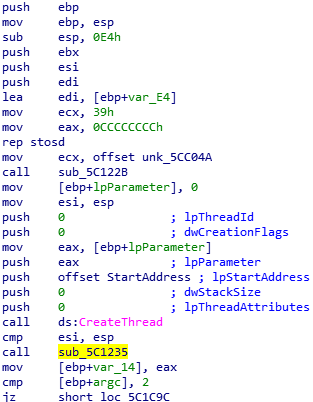
נרד עד למטה לפני הexit\_code וניכנס לפונקציה sub\_412550 (הזו שאחרי נוסתה והיא לא הmain):



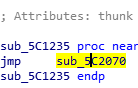
כאן כמובן אנו רואים את שלושת הפרמטרים המועברים לmain. ניכנס לפונקציה sub\_4112c6:



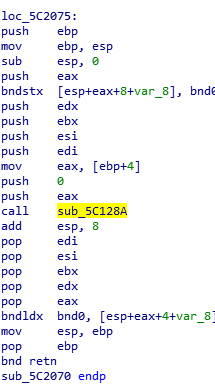
ניכנס לפונקציה sub\_411235:



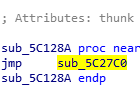
ניכנס:



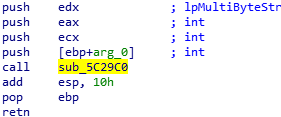
כנ"ל:



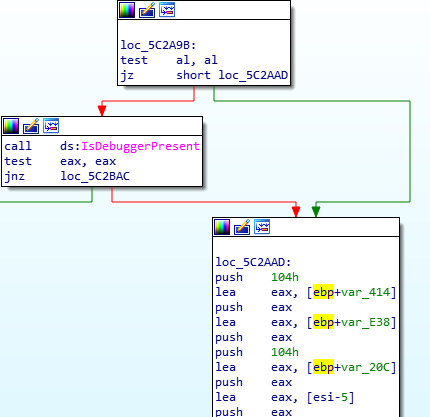
ניכנס לפונקציה sub\_5C128A:



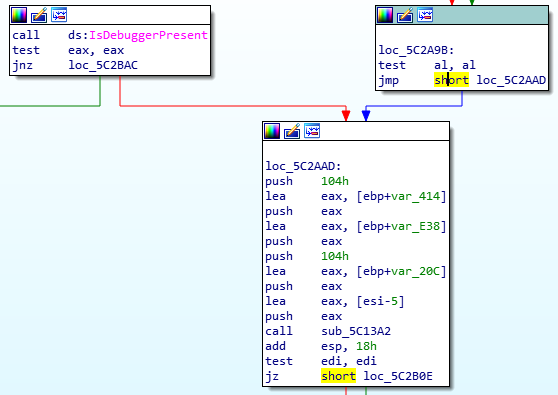
כנ"ל:



כפי המתואר בתמונה האחרונה, נכנסנו לפונקציה sub\_5C27C0 ולאחר מכן ירדנו עד למטה לפונקציה האחרונה. כעת ניכנס לפונקציה sub\_5C29C0 :

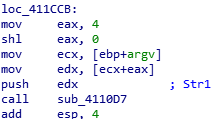


ומצאנו את האנטי-דיבאג. האנטידיבאג הוא IsDebuggerPresent.  
כדי לעקוף (כמובן) את מנגנון האנטידיבאג ניגש לloc\_5C2A9B (מוצג בתמונה האחרונה) ושם נשנה את התנאי jz short loc\_5C2AAD ל jmp short loc\_5C2AAD:

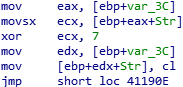


1. בשאלה זו אנו אמורים למצוא את הסיסמה שתביא לנו ציון מושלם, ללא עקיפה דרך patching.

תחילה אנו רואים כי לאחר הכנסת הסיסמה התוכנית בודקת את אורך הסיסמה.  
לאחר מכן נלך בעקבות החץ הירוק לכאן:



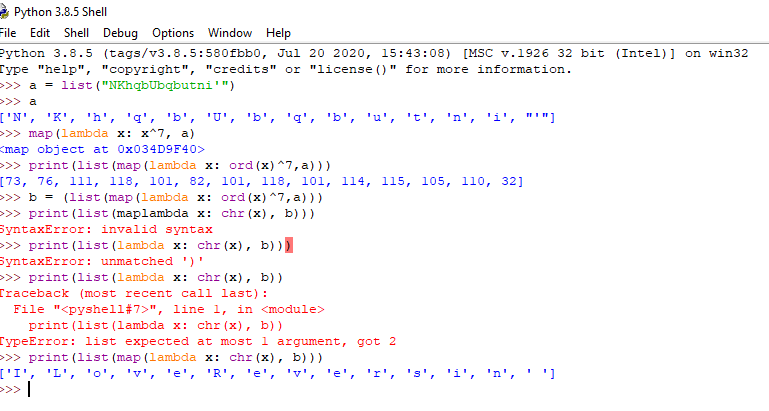
ניכנס לפונקציה sub\_4110d7 :



כפי המוצג בתמונה האחרונה כאן, אנו "מנווטים" קצת באלגוריתם של פונקציה זו בכדי לראות מה היא עושה עם המחרוזת. נשים breakpoint ונריץ, וכאשר נגיע לשלב זה נקבל את המחרוזת:

NKhqbUbqbutni'

אקח את מחרוזת זו לpython, אעשה XOR עם 7 כמו שנעשה בפונקציה ונגיע למחרוזת הבאה:



לכן המחרוזת שיצאה לנו הינה: ILoveReversing