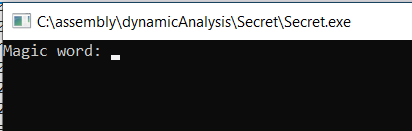
בס"ד

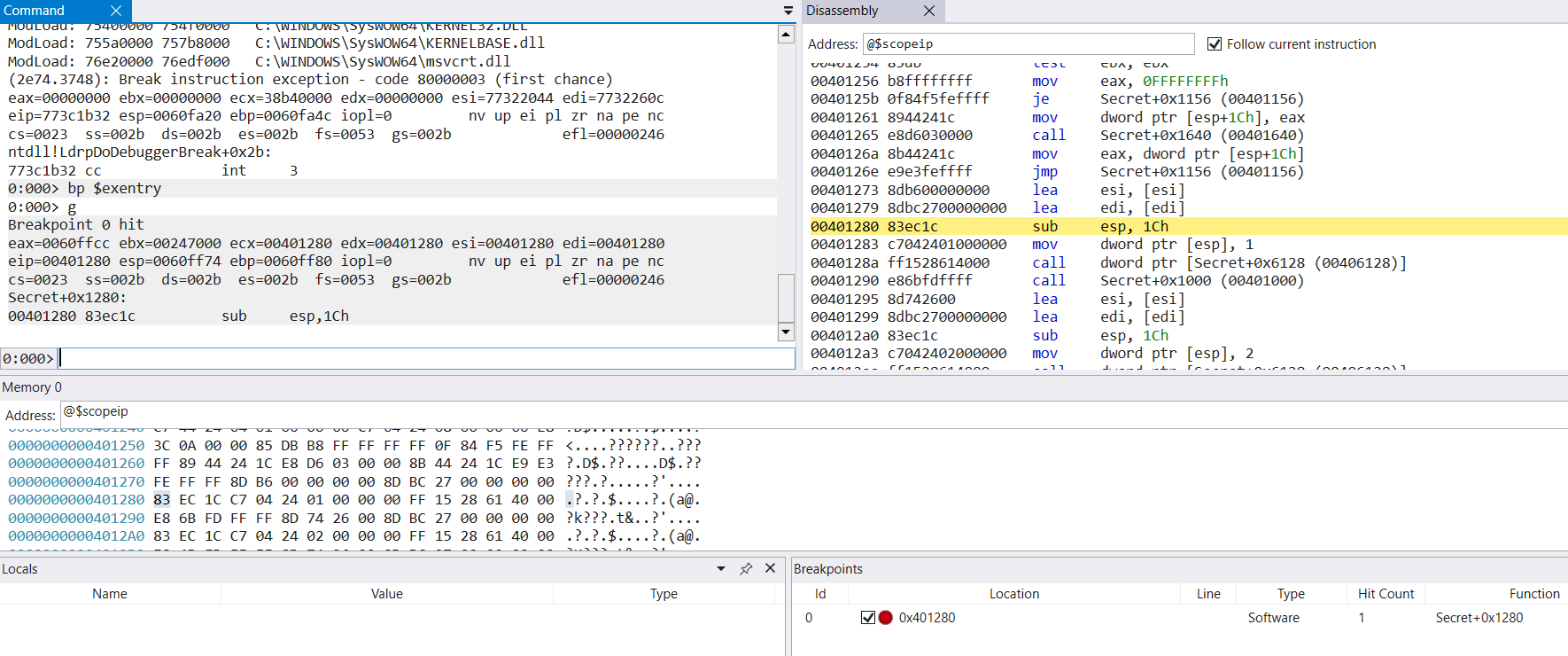
WriteUp "secret" exercise – Yishai Lutvak

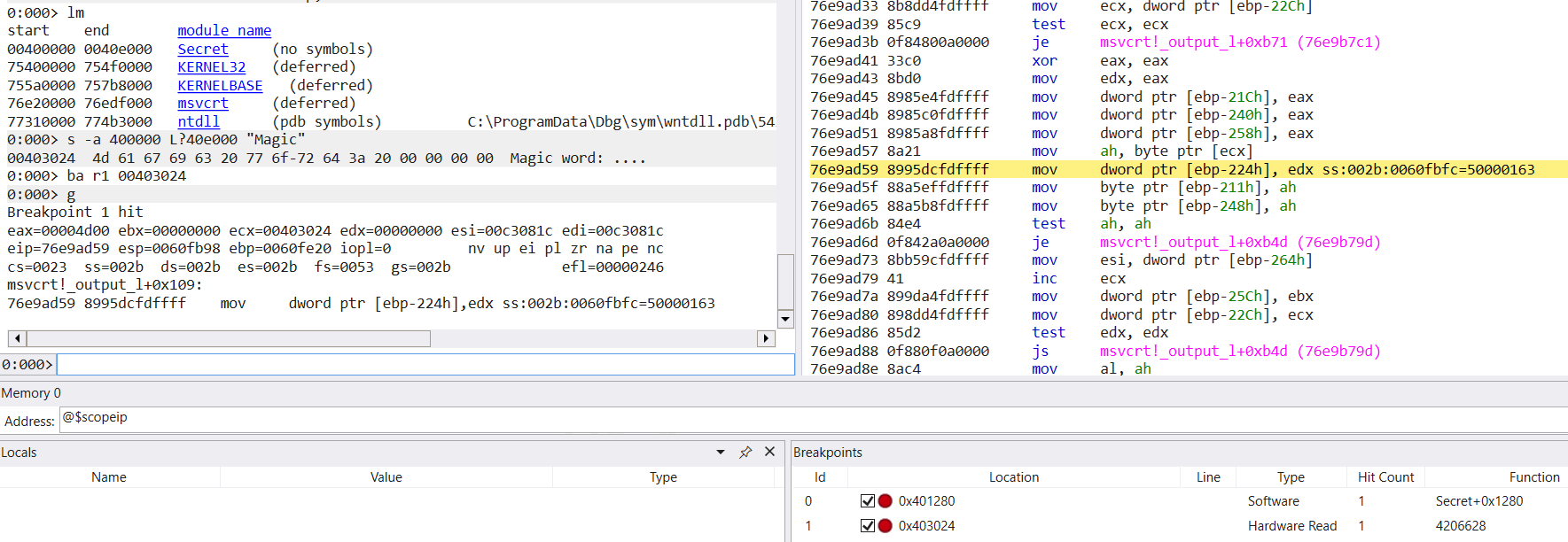
נריץ את התרגיל secret.exe בwindbg



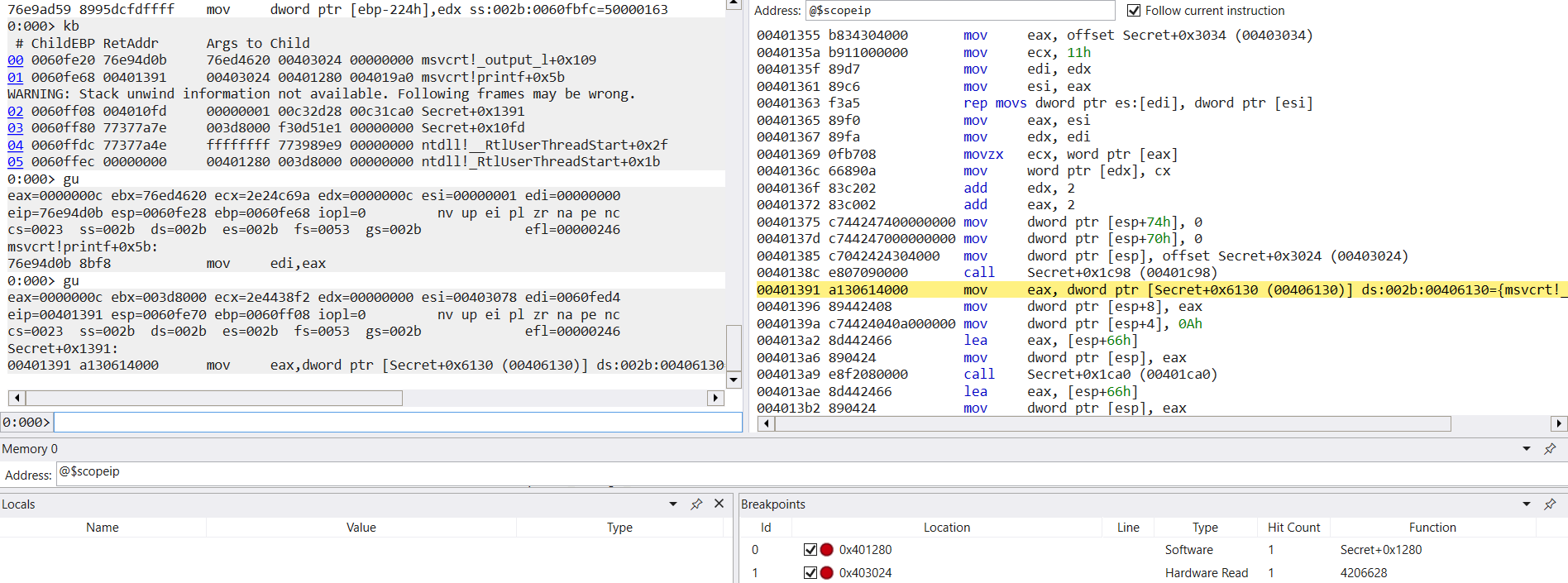
ראינו שהוא מדפיס "Magic word:"

לכן נחפש את המחרוזת הזאת ונמצא מתי ניגשים לזיכרון שבו היא נמצאת כדי לאתר את הmain.

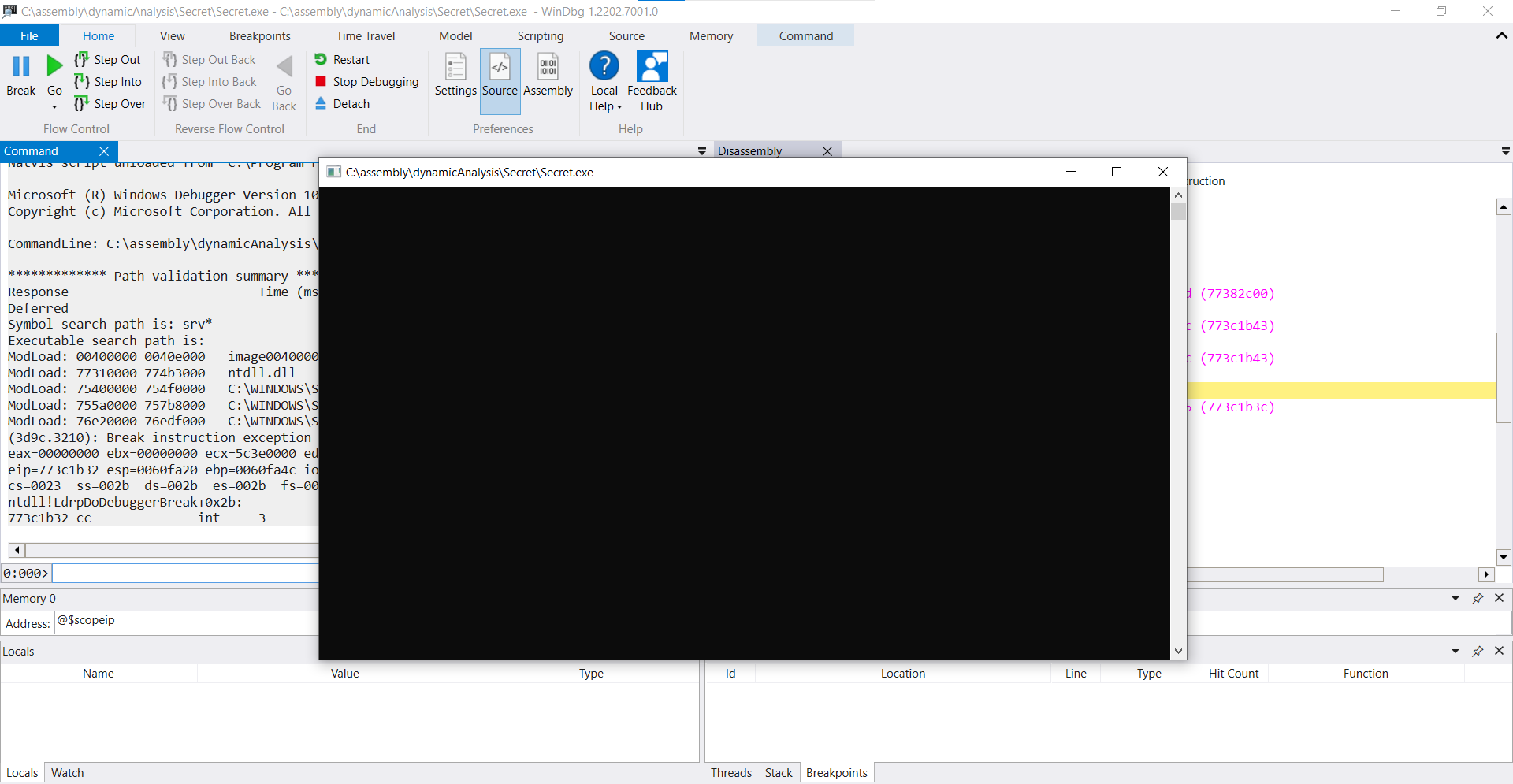




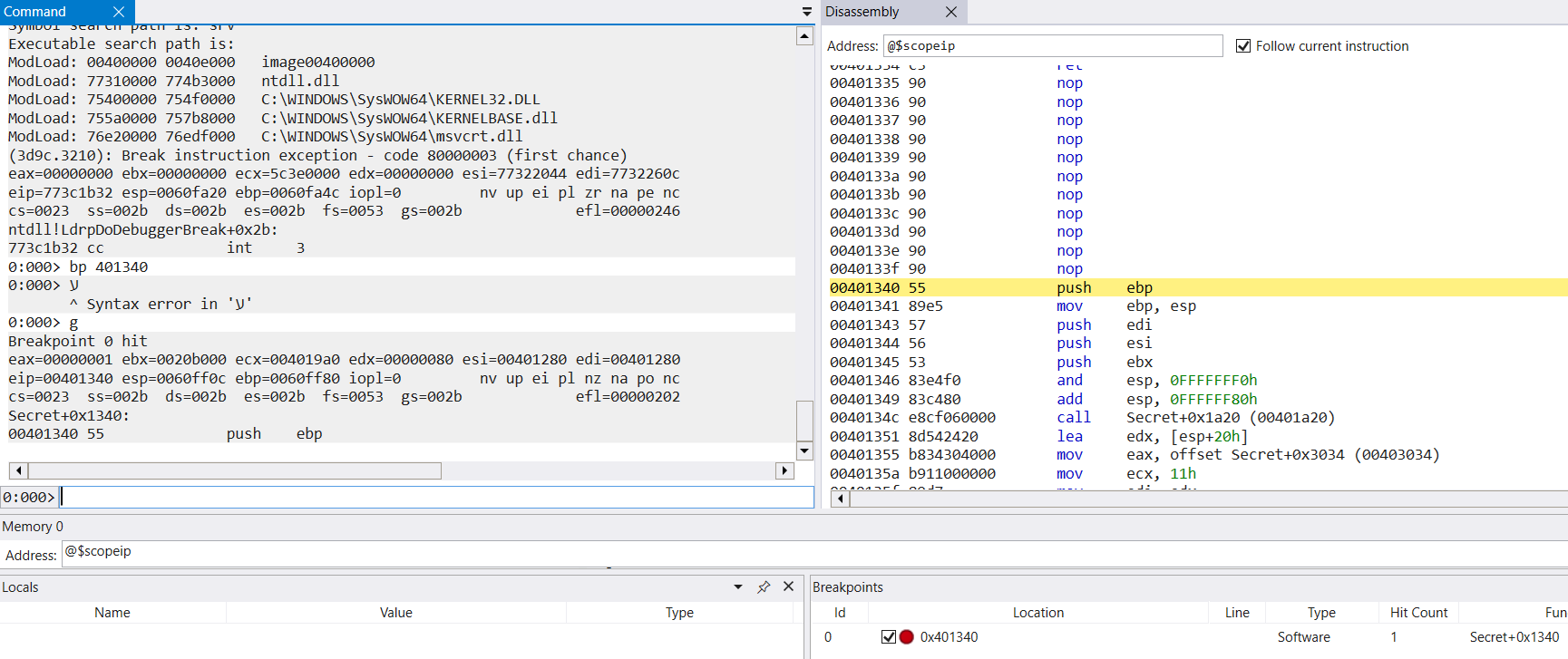
נבקש לראות את הקריאות למחסנית באמצעות הפקודה kb, אחר כך נזהה שכתובת המחרוזת המודפסת "Magic word:" (403024) מועברת כארגומנט (בפעם הראשונה) שתי רמות למעלה יותר במחסנית, כאשר כתובת החזרה היא 401391. לכן נבצע פעמיים את הפקודה gu ונגיע לmain



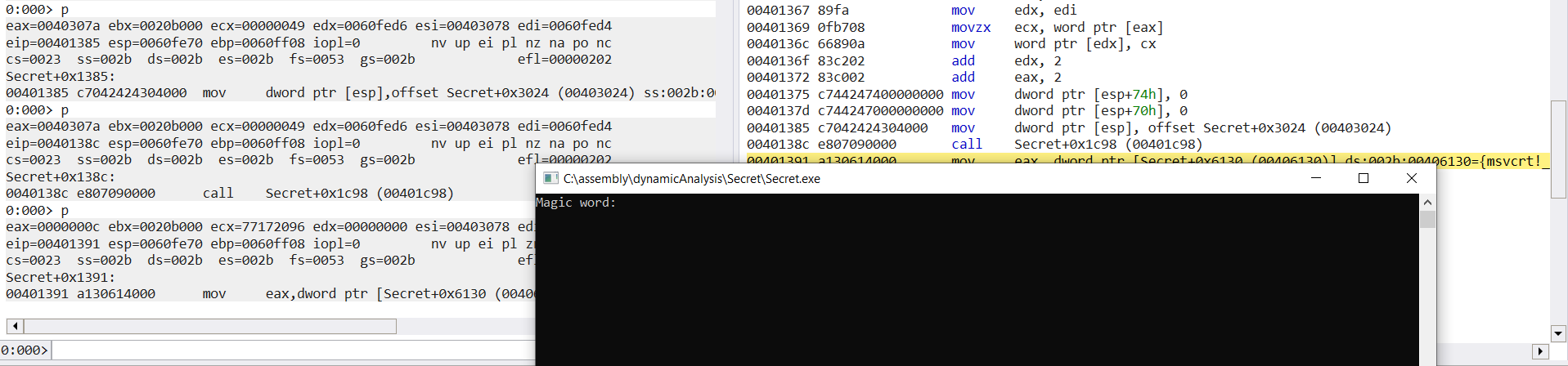
נעשה restart



נשים bp בתחילת הmain (401340) ונריץ שוב.

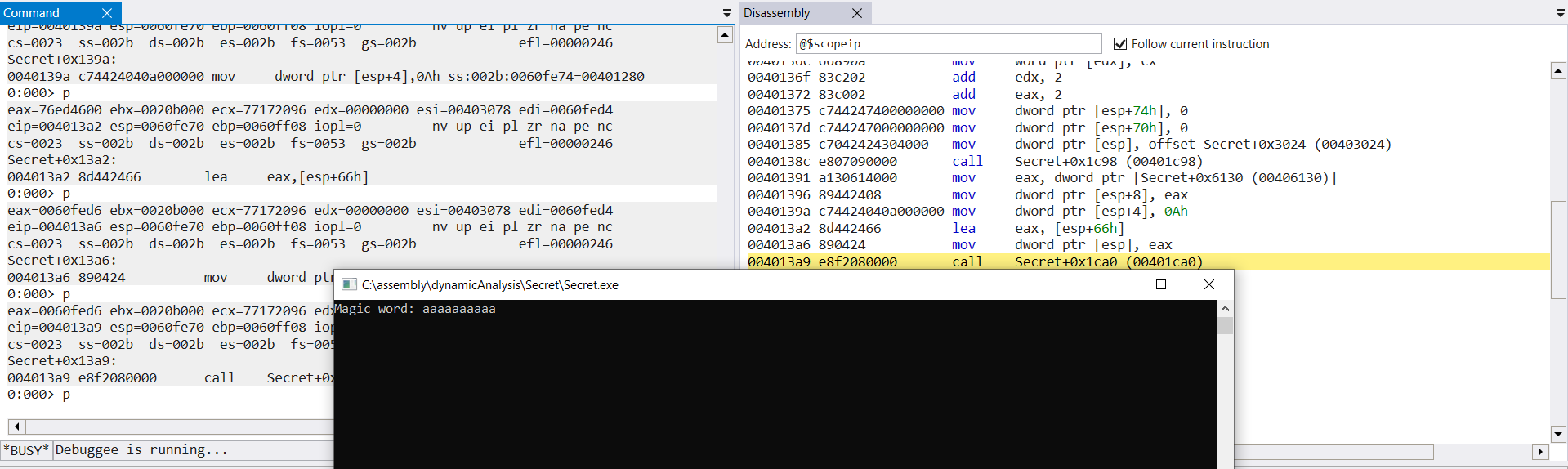


נגלה כי הפקודה call בכתובת 40138C מדפיסה למסך את ההודעה "Magic word:".



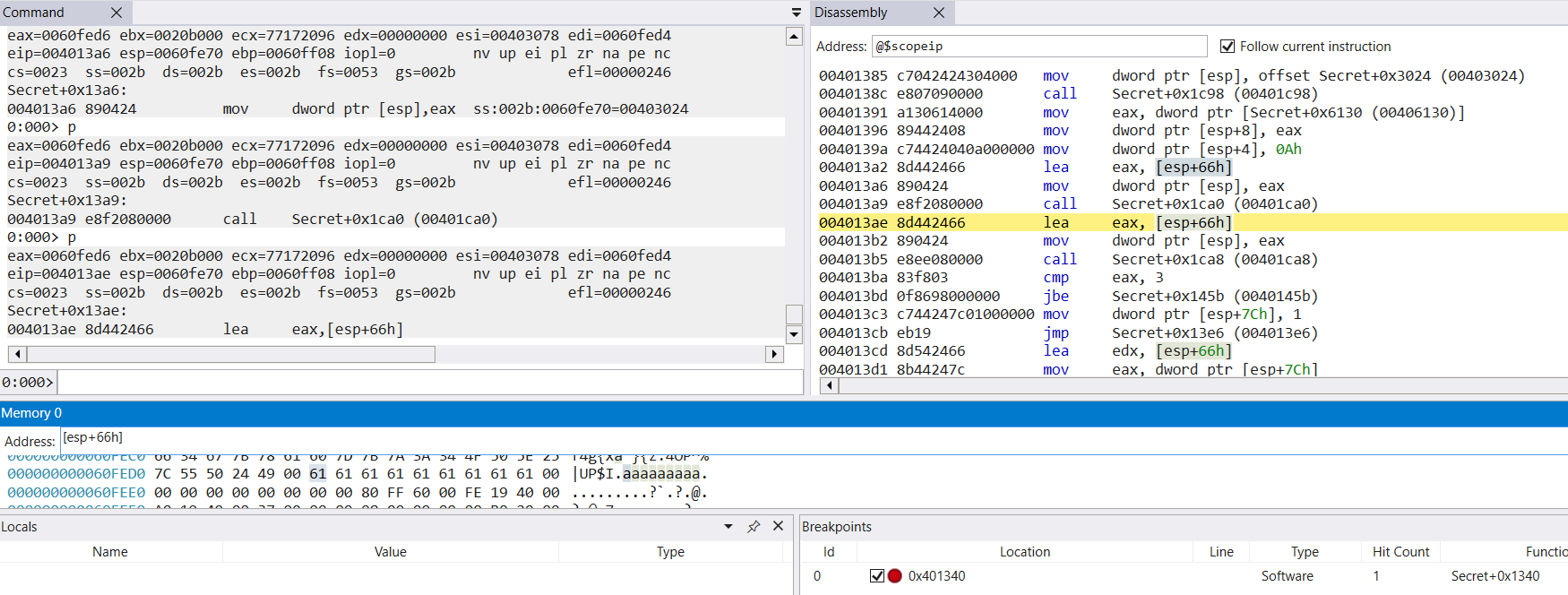
אחר כך נגלה כי הפקודה call בכתובת 4013A9 מקבלת קלט מהמשתמש

נקליד סתם משהו – "aaaaaaaaaa" (10 פעמים a)



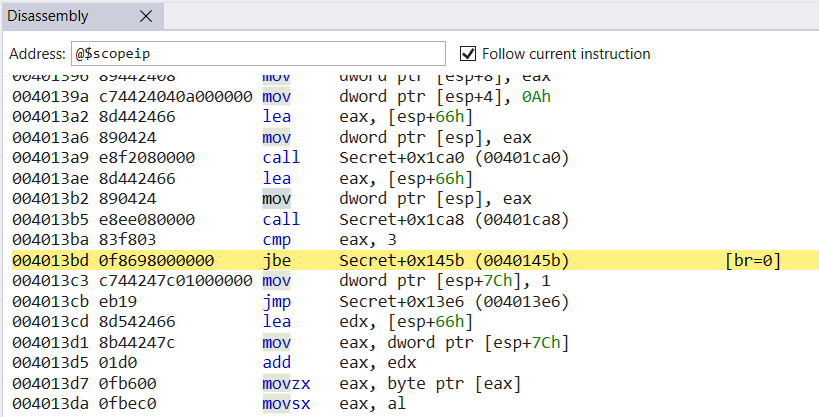
ניתן לראות את הקלט שהכנסנו "aaaaaaaaaa" בכתובת (esp+66h) כלומר בכתובת 60FED6

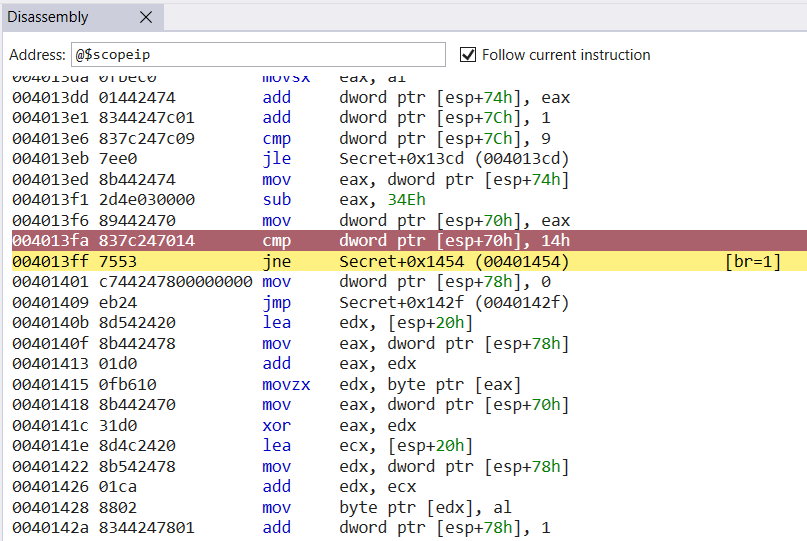
(משום מה נכנסו רק 9 a ולא 10 כמו שהכנסנו!)



נזהה שתי קפיצות שמעיפות אותנו לסוף התוכנית.

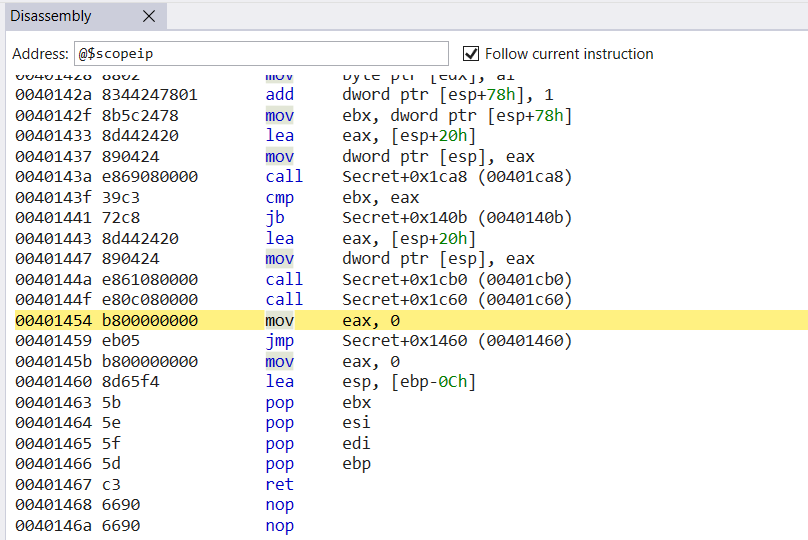
אחת בכתובת 4013BD ואחת בכתובת 4013FF:



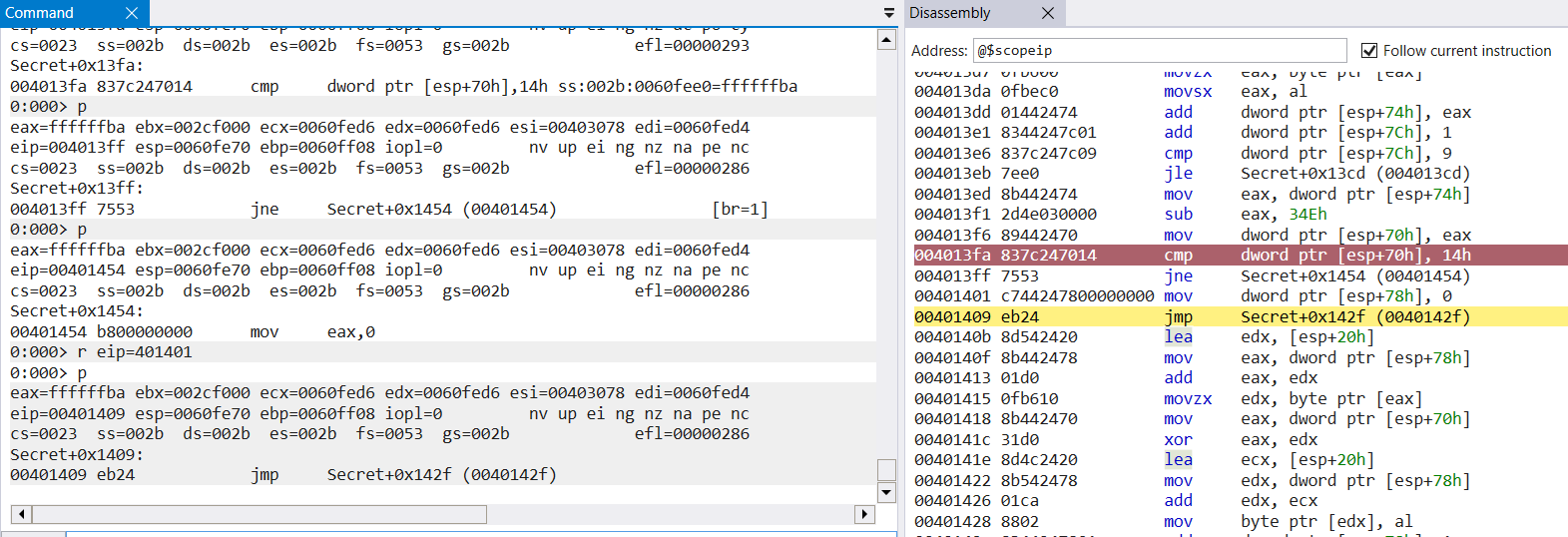


אחר כך זה נראה שאין מה שיזרוק אותנו החוצה לסוף התכנית.

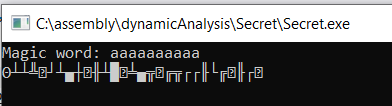
לכן ננסה לראות אם הוא מכניס אותנו לקטע שמעבר לכתובת 4013FF ואם לא אז פשוט נשנה ערכו של הרגיסטר eip.



הוא העיף אותנו לסוף התכנית. בסה. לא נורא. נשנה את ערכו של הרגיסטר eip ל401401.



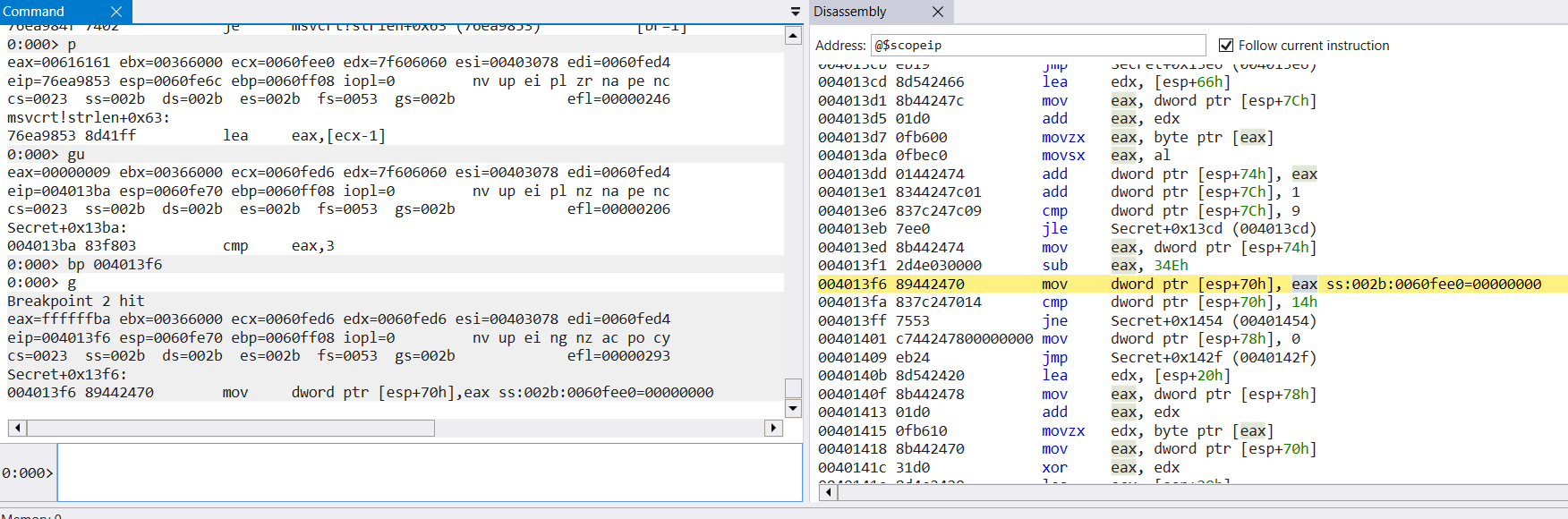
נריץ עד הסוף ונראה מה קורה..

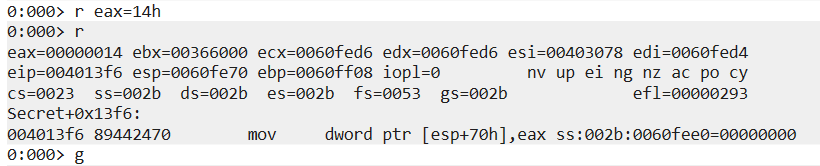


הודפס משו לא ברור. כנראה יש פה איזה מחרוזת מוצפנת ושיבשנו את הקוד שמפענח אותה איפה שהוא בדרך.

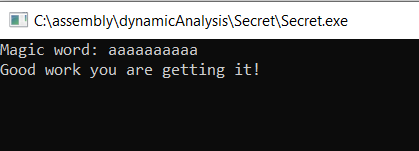
נעשה restart, נריץ עוד פעם לאט לאט, ובכל פעם שצריך נשנה את eip כדי לבצע את הפקודה שהייתה צריכה להתבצע אם היינו מקלידים את מילת הקסם.

למשל, לפני השורה המסומנת (בתמונה הבאה) אני אכניס לeax את הערך 14h, כדי שההשוואה בשורה הבאה תצא נכונה..:





והנה הצלחנו לפענח את המחרוזת המוצפנת:



לאחר מחקר נוסף והבנה של מהלך הקוד הבנתי שהמספר הסודי הוא 866 והמפתח הוא 20

|  |
| --- |
|  |
|  |
|  |
|  |

להלן קוד בפייתון המדמה את הפעולה התוכנית:

