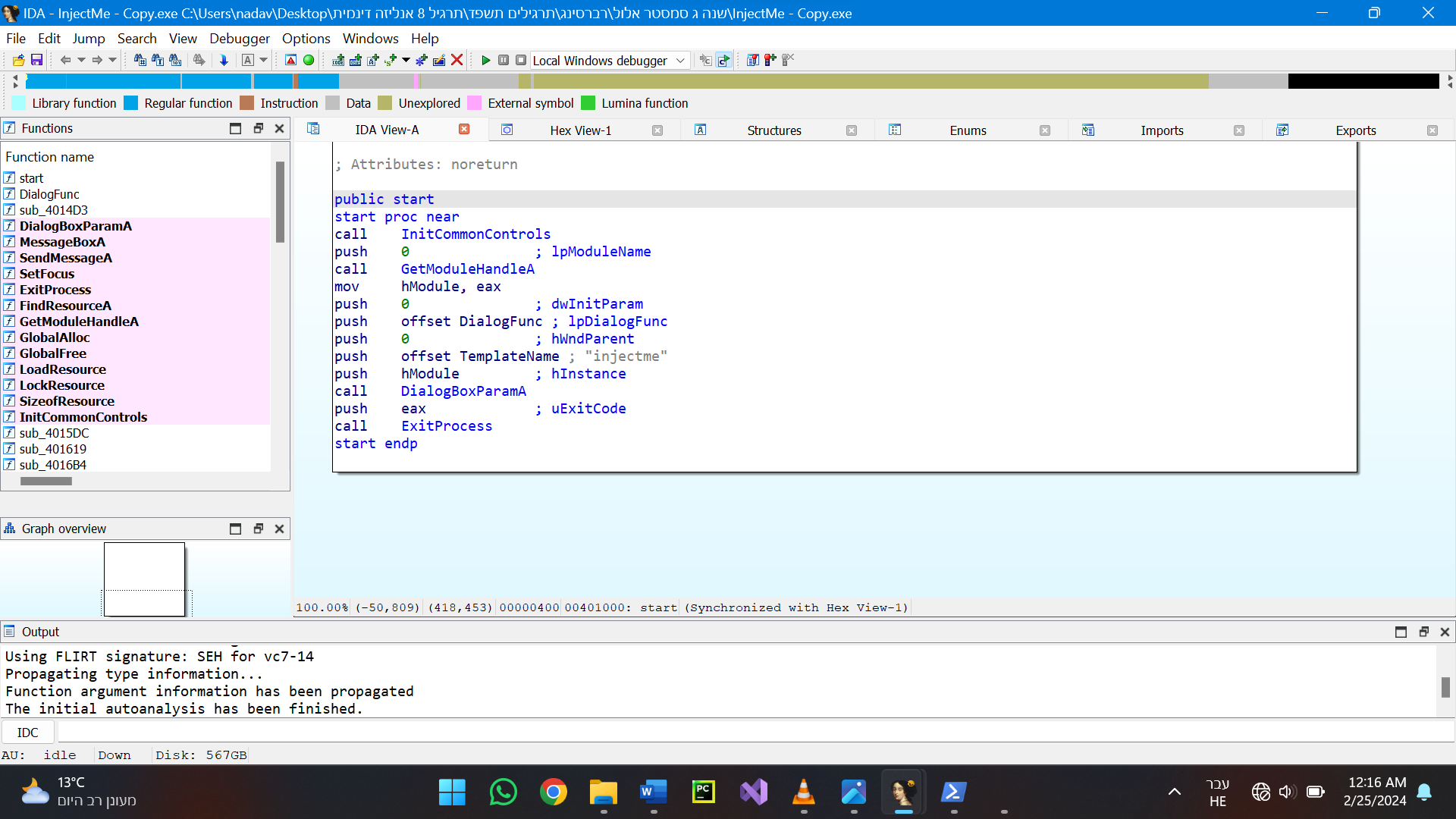
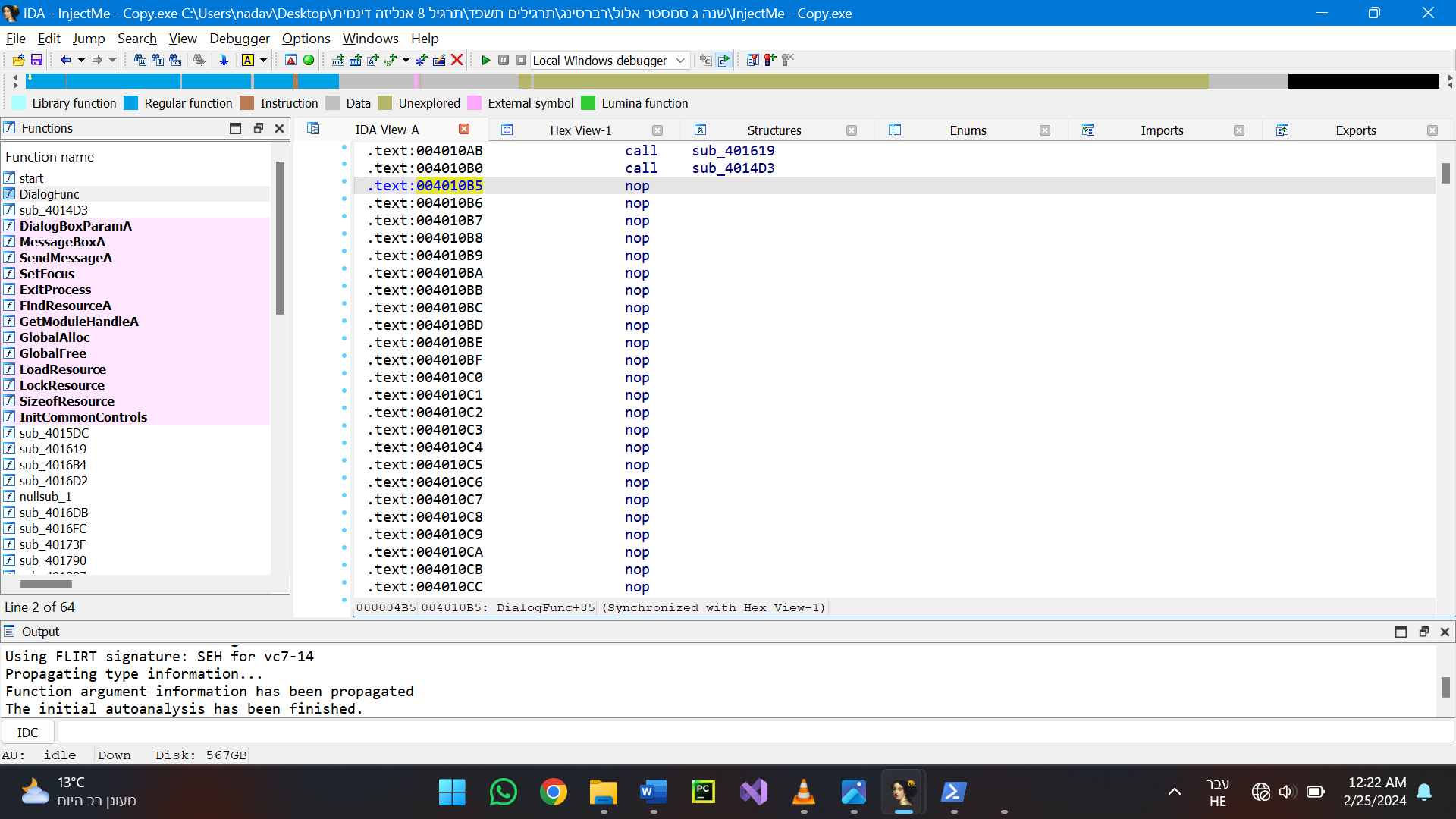
# תרגיל 8 InjectMe – נדב צימרמן

ראשית פתחתי את הקובץ "InjectMe.exe" על ידי תוכנת הדיסאסמבלר IDA כפי שביצענו בשיעורים בכיתה, על מנת לנסות ולהבין את מבנה התוכנית.

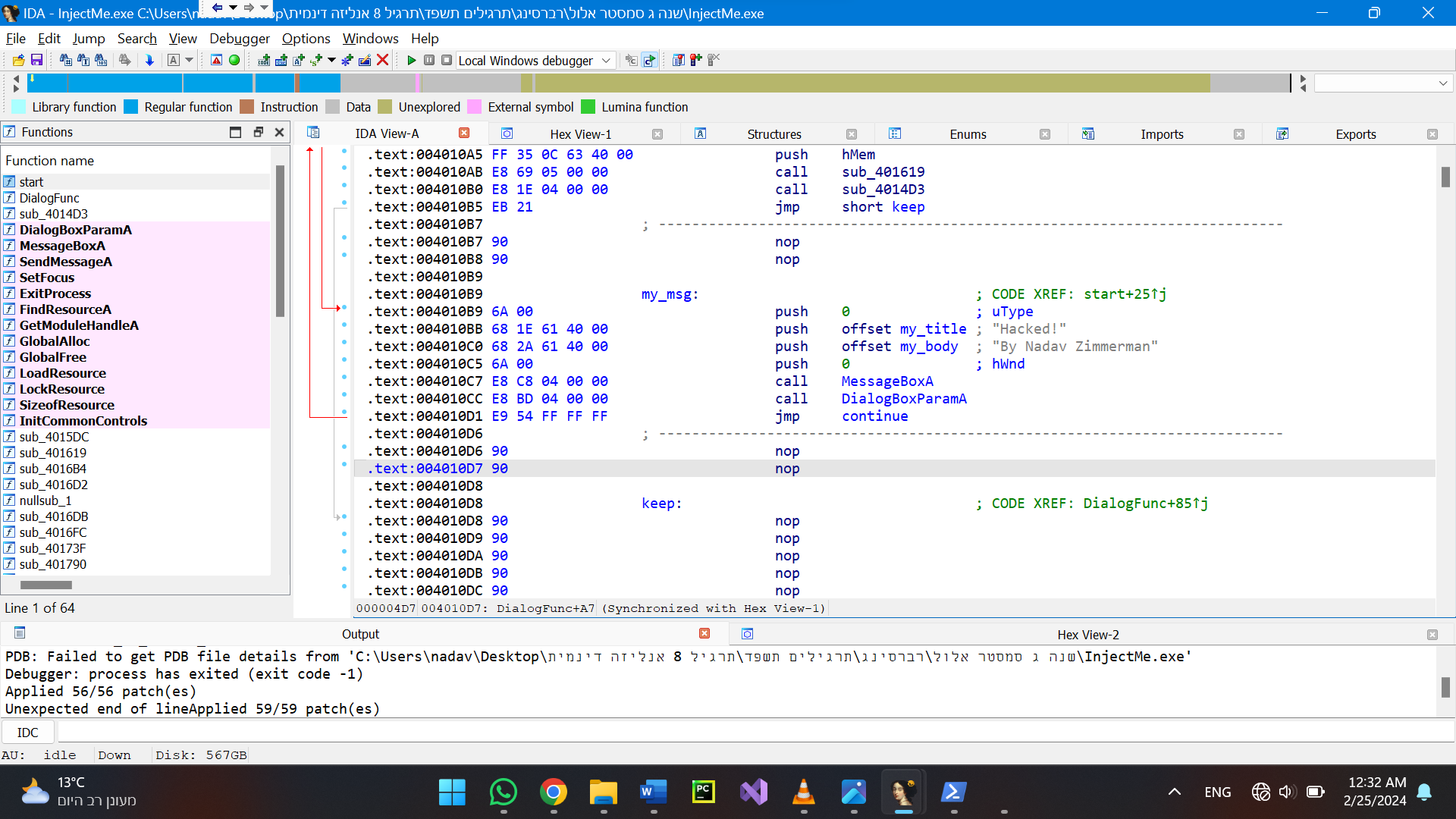
לאחר חיפוש של המחרוזת "injectme" שמופיעה בחלון שנפתח מיד בהרצת התוכנית ומספר יציאות על מנת להבין ממבט על את התוכנית, ראיתי כי התוכנית מבצעת קריאה לפונקציה DialogBoxParamA בה מתרחש הקוד הגורם להופעת תיבת "injectme" יחד עם הצליל הייחודי. אם כן ברצוננו להוסיף קטע קוד אשר יתרחש בטרם הקריאה לפונקציה זו ויגרום להופעת התיבה הדרושה, כפי שמופיע בתמונה להלן:



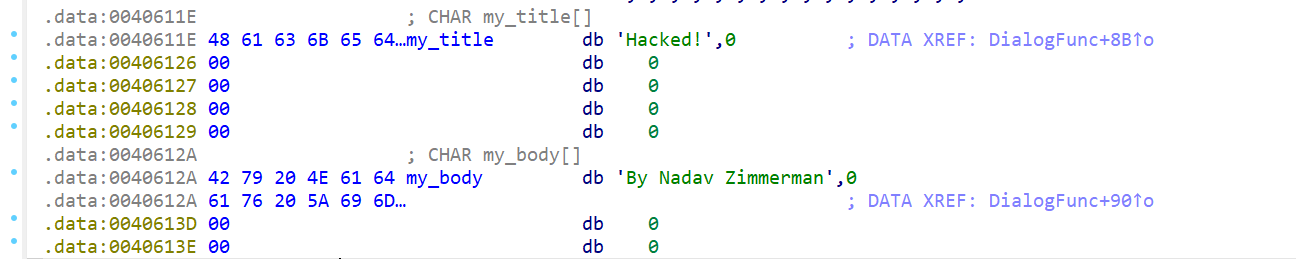
חיפשתי קטע פנוי בו אוכל להכניס patch עם קטע הקוד הדרוש ואכן מצאתי בכתובת 004010B5 רצף של nop's:



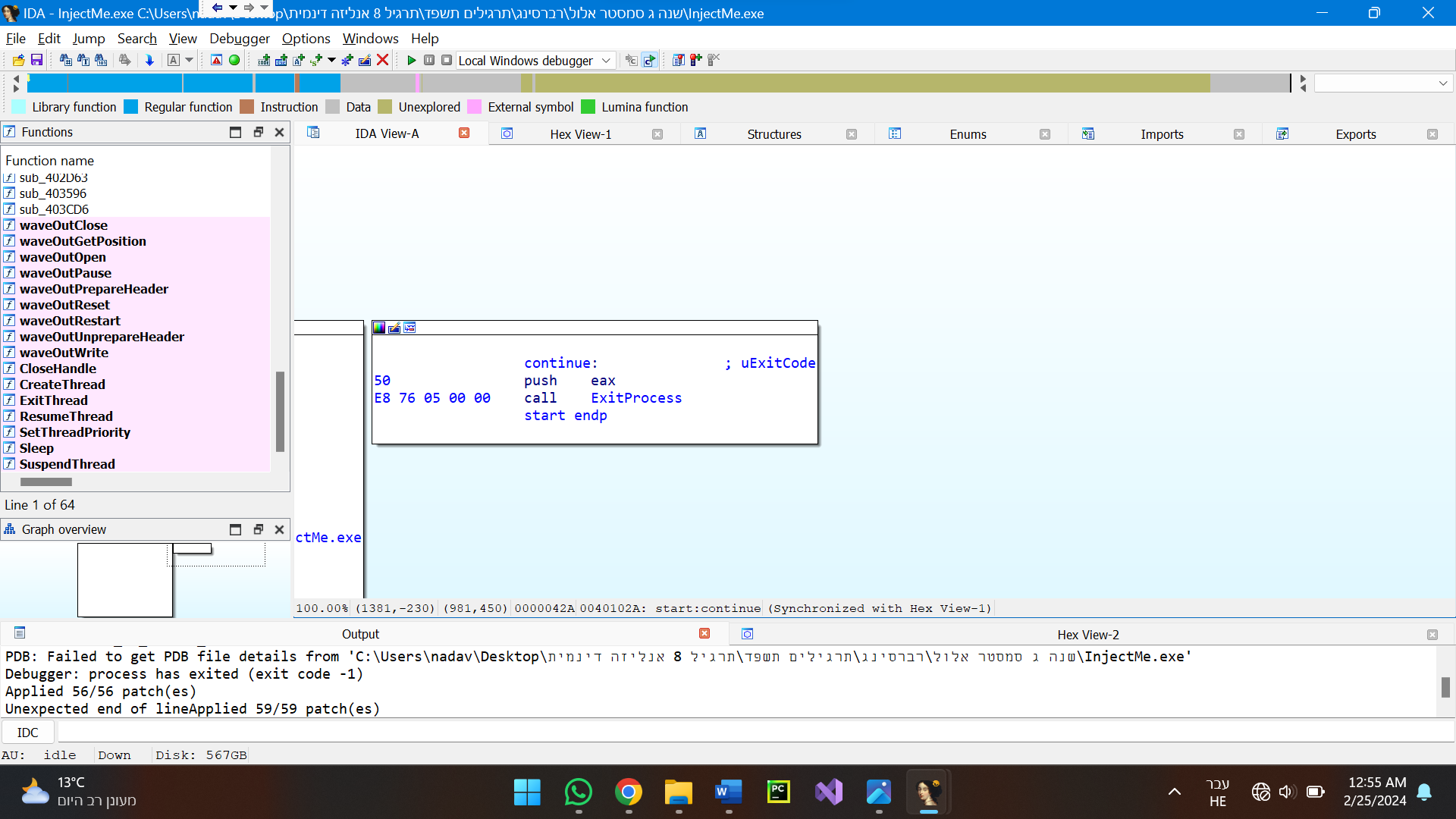
ע"פ ההנחייה לתרגיל הסתכלתי על הפונקציה MessageBoxA ולמדתי אילו פרמטרים היא צריכה לקבל. הוספתי בקטע של הnop's את קטע הקוד הבא אשר מבצע קריאה ל MessageBox עם הפרמטרים הדרושים, לאחר מכן קורא לפונקציה המקורית של התוכנית: DialogBoxParamA ולבסוף חוזר לכתובת של המשך קוד המקור כפי שניתן לראות בתמונה להלן:

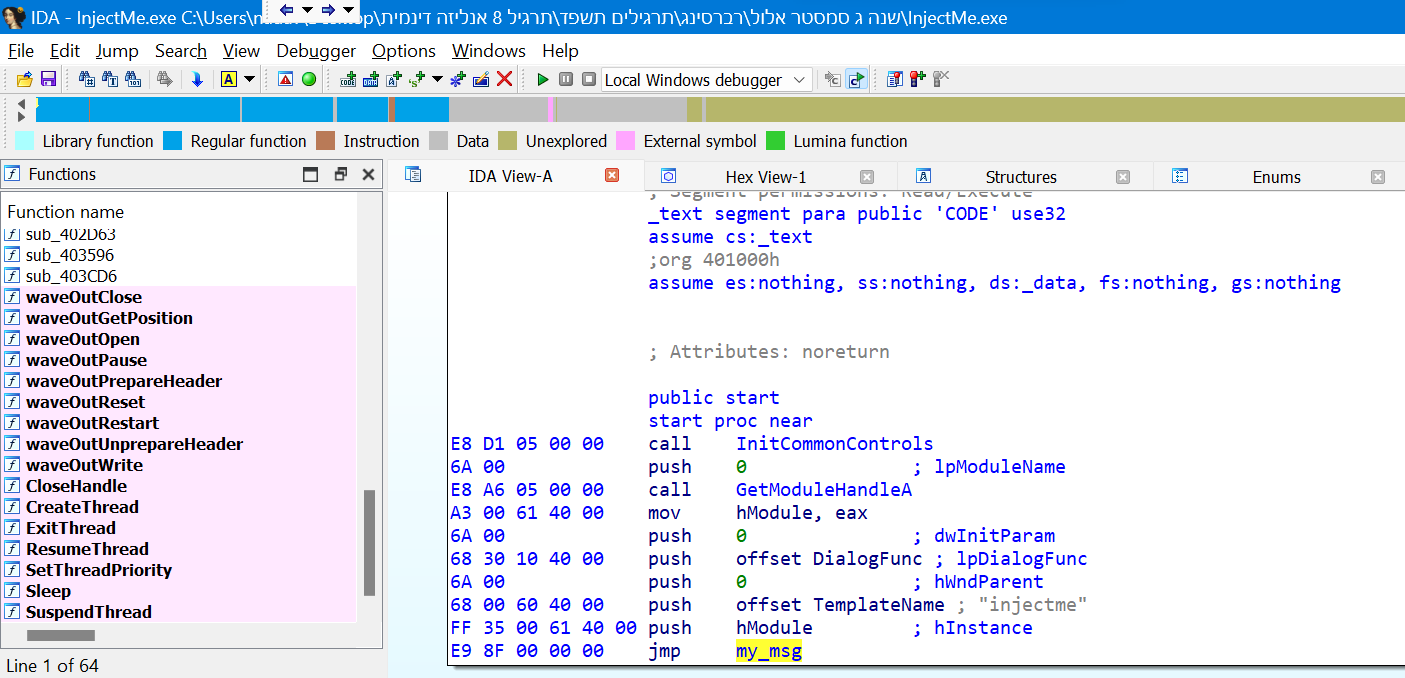


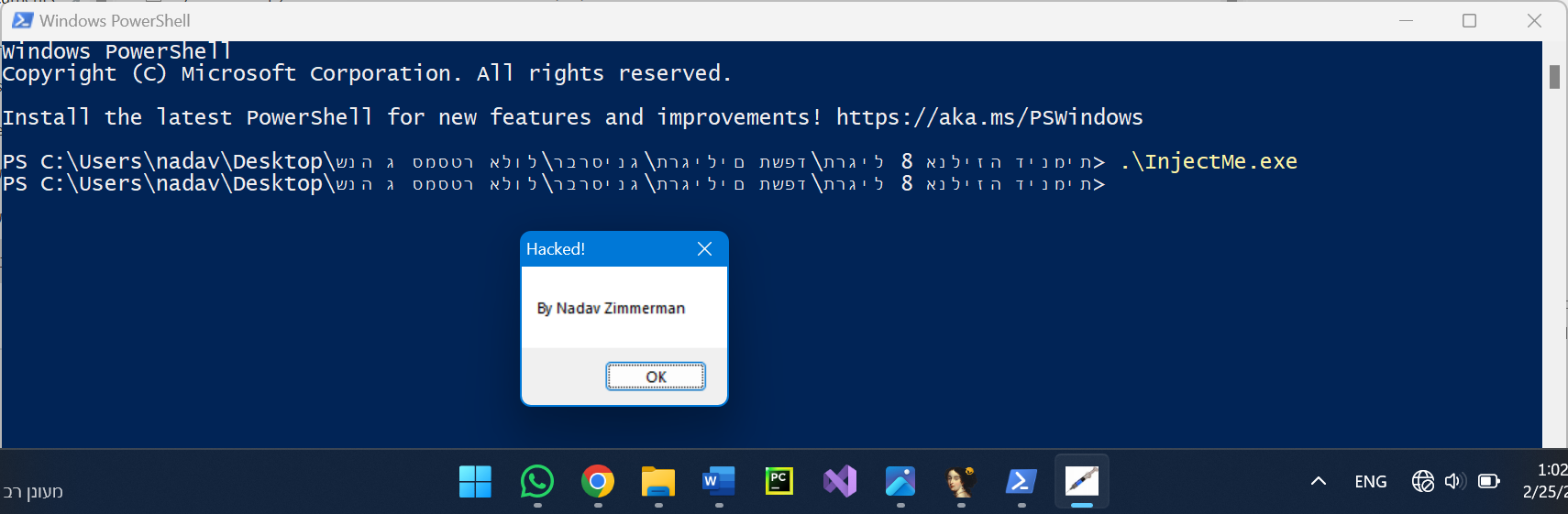
כמובן שהוספתי קפיצה מובנית (jmp keep)לפני ואחרי קטע הקוד כך שהקוד המקורי של הnop's ידלג על קטע הקוד שהוספתי.

כפי שניתן לראות בתמונה הקודמת לצורך יצירת תיבת ההודעה הוספתי בחלק של הdata שתי מחרוזות השומרות את הטקסטים של הכותרת והגוף של התיבה של ווינדווס:



לבסוף, שיניתי את קוד המקור כך שיקרא לקטע הקוד שלי במקום לפונקצייה המקורית, תוך הוספת תווית אליה תחזור התוכנית:



וכך קיבלתי את הדרוש: