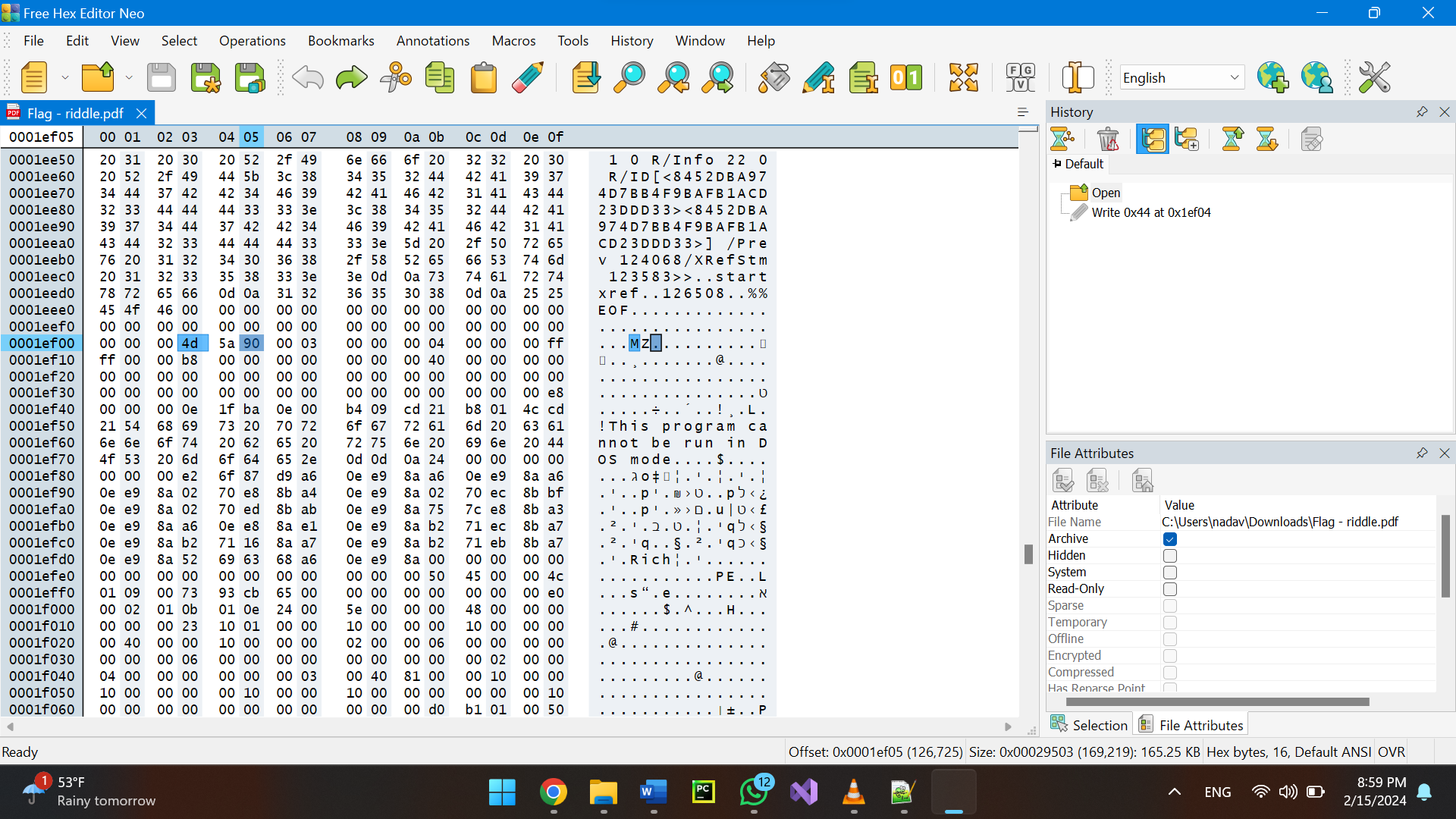
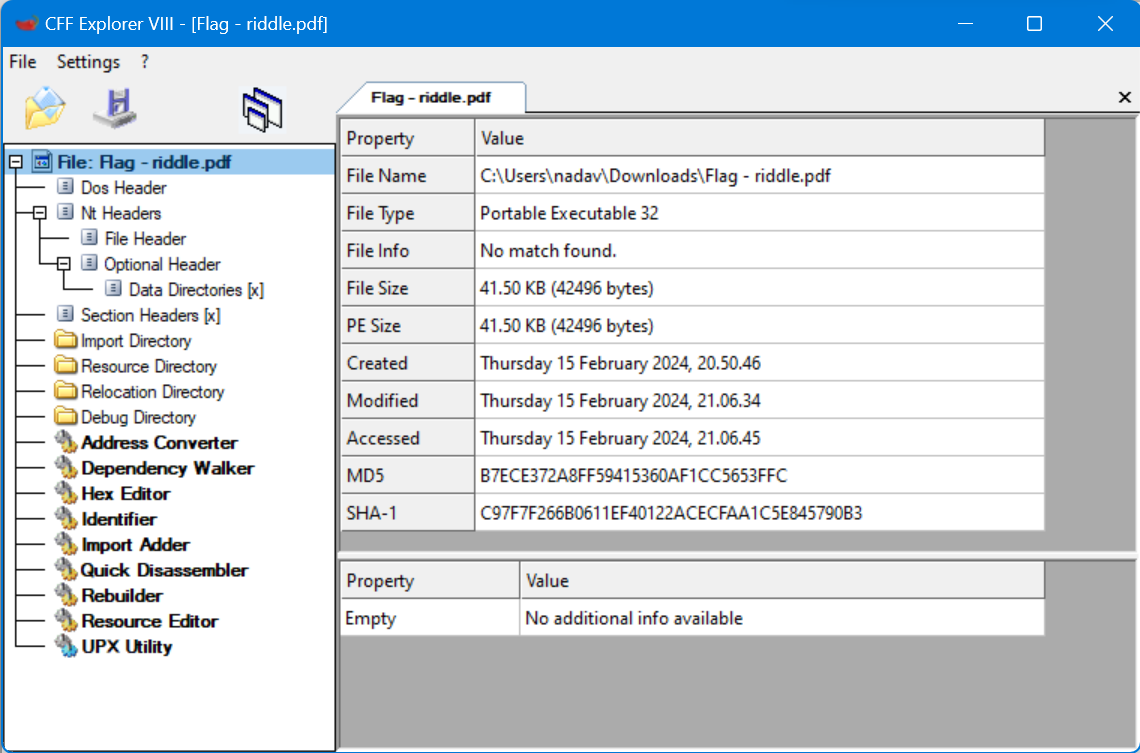
# תרגיל 7 FLAG – בנושא קבצי PE ואנליזת קוד – נדב צימרמן

למדנו בשיעור שניתן להריץ קבצי PE וכל קובץ כזה צריך להתחיל בתווים "MZ". לכן בתחילה חיפשתי דרך להפוך את התווים הראשונים בקובץ לתווים אלו, שמסמלים את תחילת הקובץ בפורמט PE.   
חיפשתי בקובץ אחר התווים הללו בתוכנה "Free Hex Editor Neo" ומצאתי אותם בשורה 001ef00 (ולאחריהם המשך הקידוד של קבצים נוספים בפורמט PE שבחנתי), כפי שמופיע בתמונה להלן:

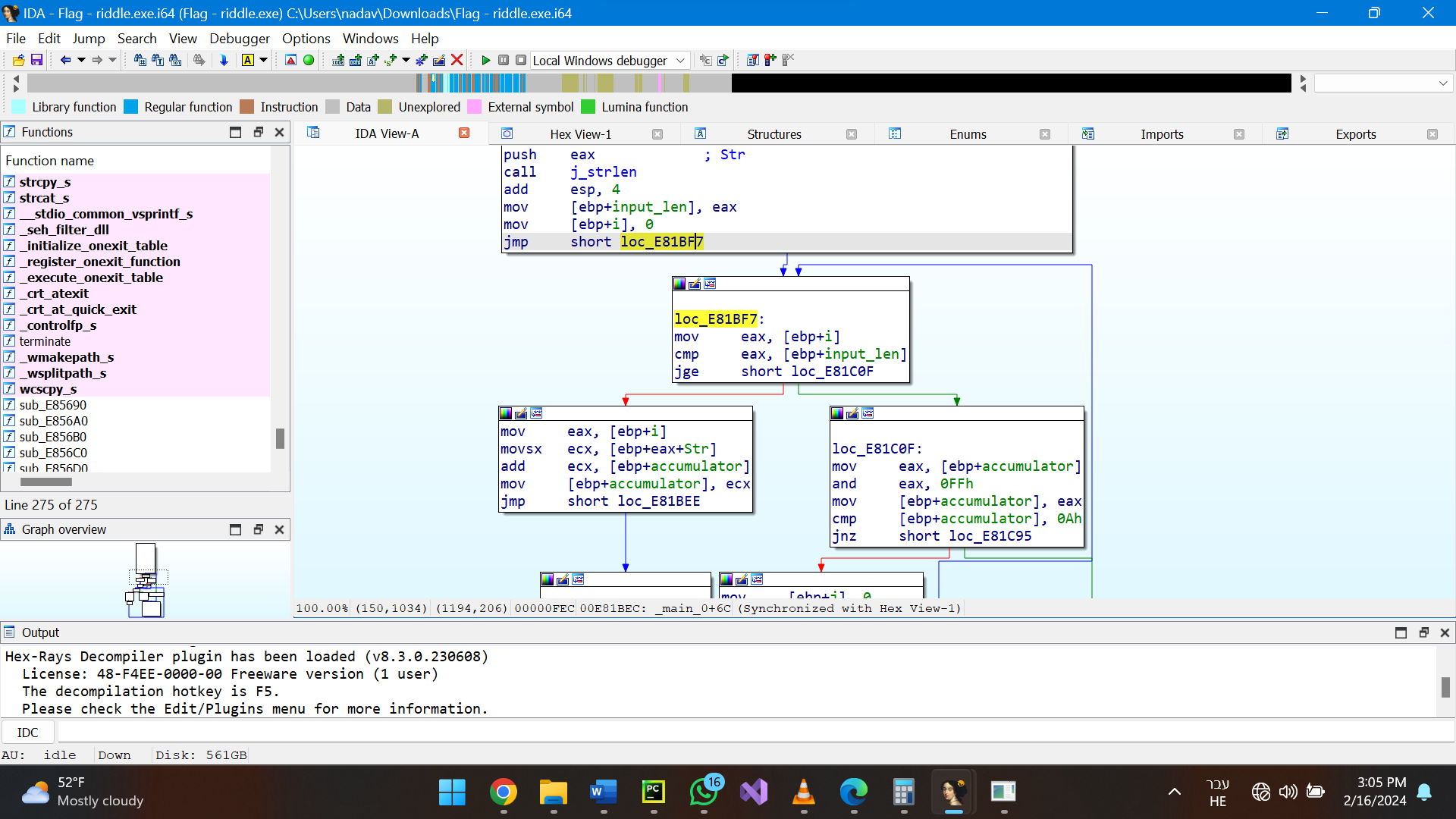


מחקתי את כל התווים בתוכנית עד לשורה זו, פתחתי בתוכנה "CFF"המרתי לסיומת exe וראיתי כי התקבל קובץ בפורמט PE:

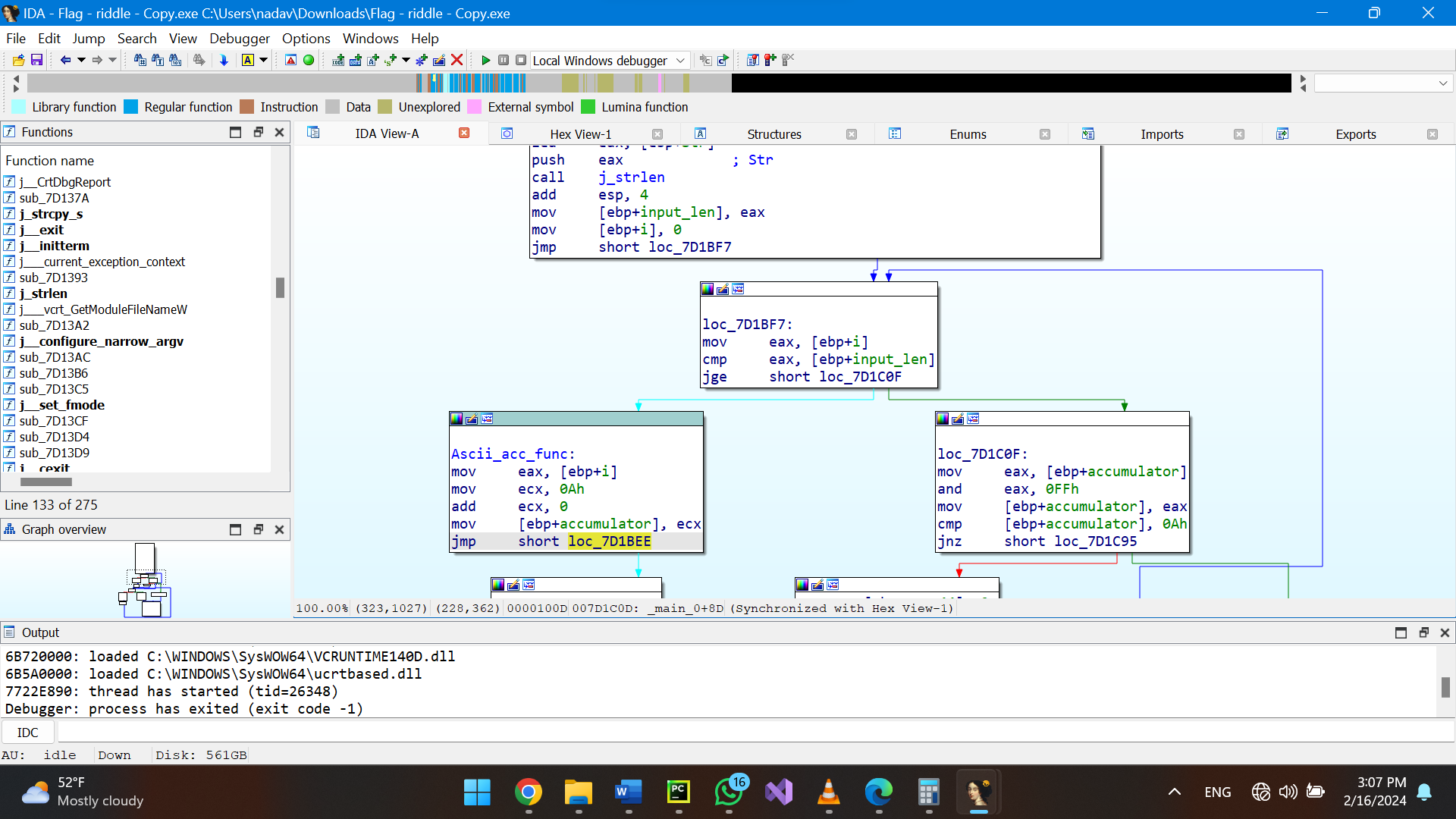


אם כן קיבלנו קוד exe בפורמט PE שניתן להרצה.

בשלב הבא נפענח את הקוד, בעזרת סביבת העבודה IDA.

 ניתן לראות שבשורות המובאות להלן בתוכנית, התוכנית סוכמת את ערכי הAscii של הפלט שהתקבל ומשווה אותם למספר ההקסדצימלי A"”.

אנו רוצים כי התוכנית תדפיס את הדגל עבור כל קלט שיתקבל, לכן הוספתי patch שבמקום לסכום את ערכי הascii פשוט ידחוף 10 למשתנה הצובר כך:

(השורות של הpatch מסומנות באדום)



לאחר הרצת התוכנית התקבל הדגל: PE format, you got it!

