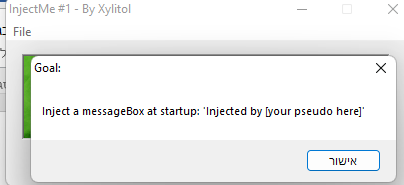
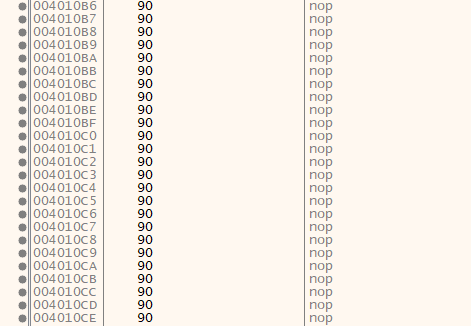
פתרון INJECTME

רז אברג'ל

המטרה של התרגיל היא לגרום לתוכנה לפתוח חלון שיפתח לפני החלון הראשי של התוכנה ושבחלון יהיה כתוב את השם שנרצה בתוספת למחרוזת הנ"ל

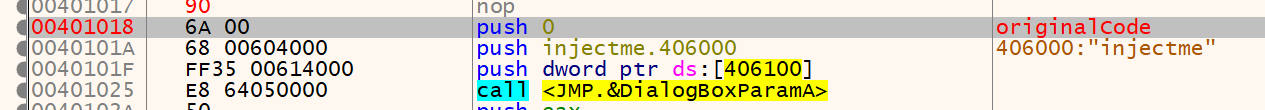


על מנת לעשות זאת נצטרך להוסיף קוד משלנו נצטרך לזהות איפה יש לנו אזור בקוד שנוכל לכתוב בו את הקוד ונראה את האזור שיש בו פקודות רבות של NOPים



לפני שנשנה את הקוד נרצה ליצור שני תגים שישמשו אותנו בקפיצות לאזור הקוד החדש ובחזרה לסדר הקוד המקורי (לפני השינוי נזכור שדרסנו את הפקודה )

(הלייבל לחזרה יהיה למעשה לפקודה אחת אחרי הפקודות שדרסנו כיוון שאת הפקודות שדרסנו נשלים לפני הקפיצה חזרה לקטע קוד זה)



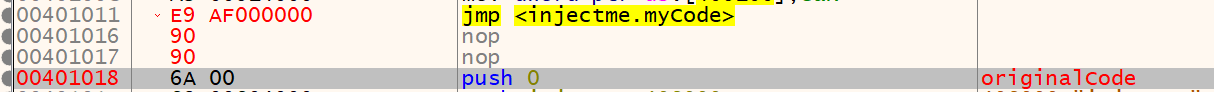
וכן לייבל באזור הnop שם נכתוב את הקוד שלנו



נבצע קפיצה לאזור הקוד הרצוי במקום הפקודה push ונזכור שצריך לכתוב שוב את הפקודה שדרסנו כשנחזור לקטע שממנו קפצנו (push 0)



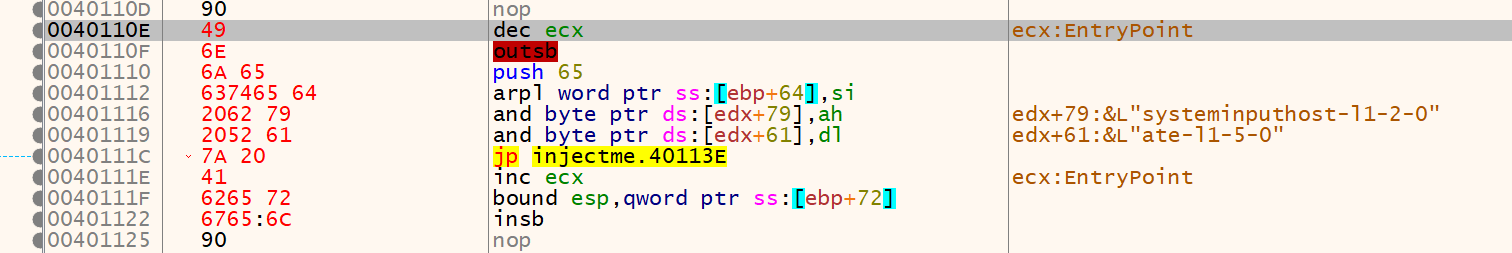
) למעשה אנחנו דורסים פה את הפרמטר הראשון ואת הפרמטר השני שנשלח לפונקציית ה(messageboxA



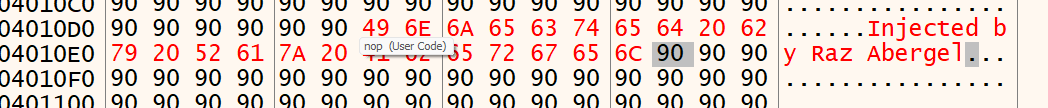
עכשיו נרצה להכניס במרחב הNOPים את המחרוזות שישלחו כפרמטרים לפונקציה של

MESSAGE BOXֹ ) נוסיף עוד מחרוזת שתהיה הכותרת של ה (message box

האזור ששנינו:



התווים כפי שהם נראים בזיכרון



ולא נשכח להוסיף בסוף המחרוזת תו של **TERMINAL NULL** שמודיע למחשב על סוף מחרוזת.



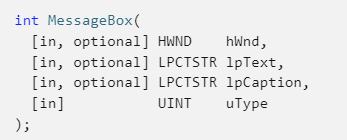
בשלב זה ניצור תג לכל מחרוזת ובעזרת התג דחוף את המחרוזת בתור פרמטר לפונקציה

Header לאזור שמכיל את הכותרת

String לאזור שמכיל את המחרוזת.

עכשיו נכתוב את הקוד באזור שלנו

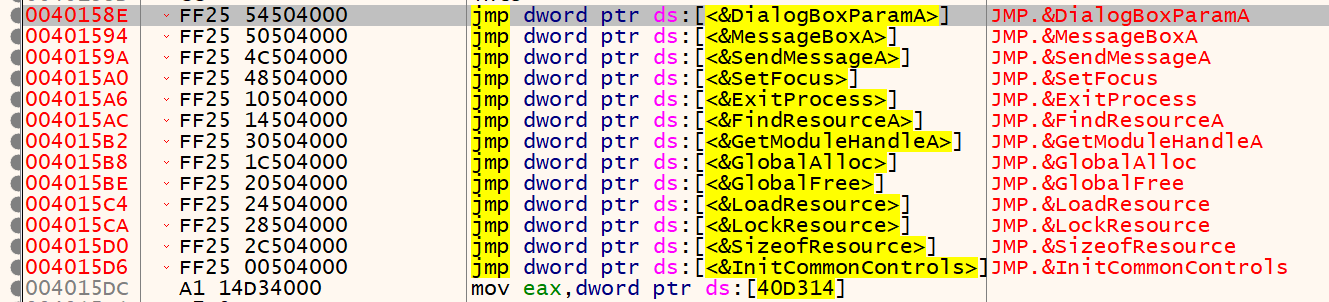
הפונקציה message box לפי msdn מקבלת 4 פרמטרים



הפרמטר הראשון והשני חשובים לנו מכיוון שאחד מקבל את הכותרת של קופסת ההודעה ואחד את המחרוזת שמודפסת בתוך הקופסה

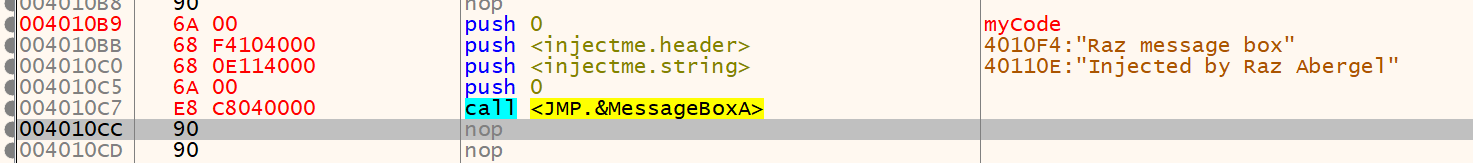
חשוב לציין כי בקריאה לפונקציה של הmessage box נהיה חייבים לקרוא לכתובת שמכילה את הקפיצה לפונקציה עצמה ולא קריאה ישירה לפונקציה וזאת מכיוון שקבצי dll מקבלים את הכתובת שלהם בזמן ריצה ובכל טעינה הloader יקצה להם כתובת וירטואלית אחרת ולכן אם נקרא לפונקציה עצמה אומנם זה יעבוד באותו רגע שנריץ אבל בהרצה הבאה הפונקציה תקבל כתובת אחרת והפתרון לא יעבוד

מכאן שנבדוק מה כתובת הקפיצה שמובילה לפונקציה שיוצרת message box



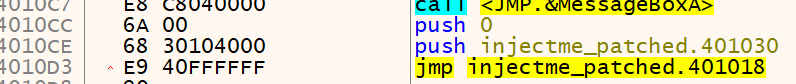
ונראה כי נצטרך לקרוא לכתובת 

נבצע את הקריאה לפונקציה

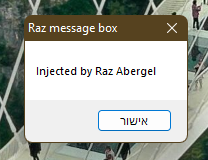


ולפני החזרה לקוד המקורי נוסיף את הפרמטרים שדרסנו בהתחלה

Push 0 and push 401030



נריץ את התוכנית ונראה שזה עובד לנו



וסיימנו.