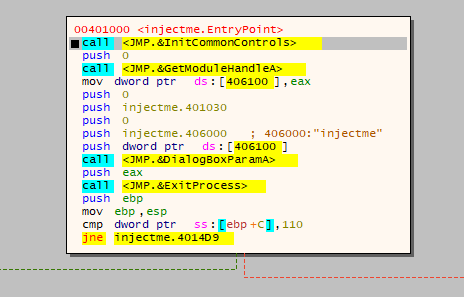
בס"ד

**ישי לוטווק InjectMe.exe הדרך לפיתרון**



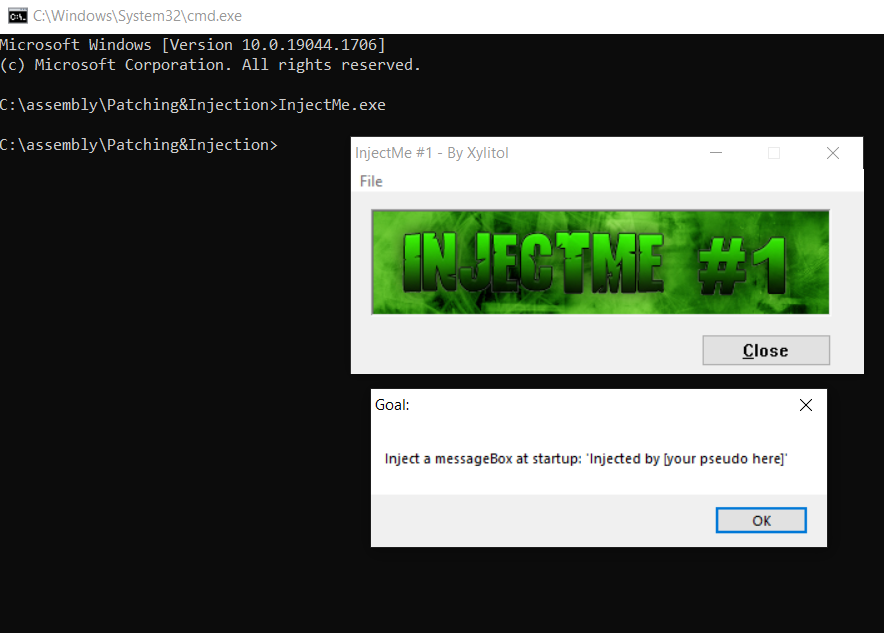
כדי לעשות את מה שנתבקשנו, נצטרך לקפוץ למקום אחר בקוד, ולחזור לפה לאחר מכן.

נבחר לפצפץ את הפקודה push 0 בשורה החמישית. כמובן שנצטרך אחר כך לשתול את הפקודה הזאת בקטע הקוד שנזריק במקום אחר, וזאת בכדי שהתוכנית תוכל להמשיך לעבוד כמצופה.

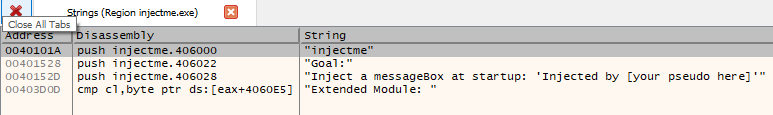
נמצא מקום ריק באזור של הקוד שבו נוכל לשתול את ההזרקה שלנו:



ננסה לראות איך מבוצעת הקריאה לפונקציה MessageBoxA שכבר נמצאת בקוד:

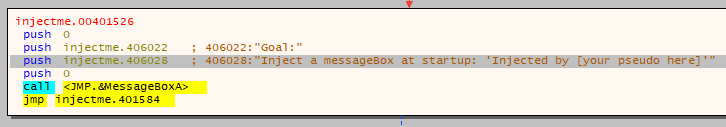


נמצא את הטקסט המודפס בהודעה:



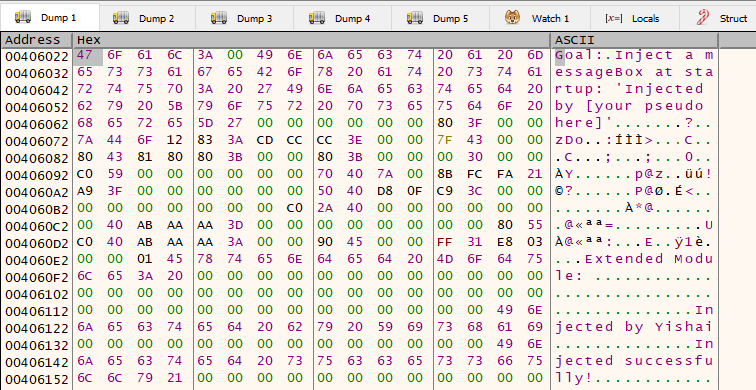
ניתן לראות את ההודעה בשורה השלישית..

נלך לאזור הזה בקוד ונראה איך מזמנים את הפונקציה הזו:



נעשה אותו דבר רק שנשנה את הכתובות לכתובות בהן נכניס את המחרוזות שאנחנו רוצים להדפיס

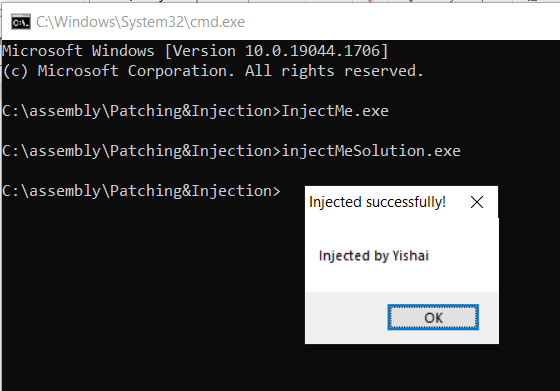
(ניתן לראות בתחתית התמונה את המחרוזות אותן שתלנו באזור של הdata):



להלן הפיצפוץ:

|  |  |
| --- | --- |
| לפני | אחרי |
|  |  |
| לפני | אחרי |
|  |  |

והתוצאה כמצופה:



ואחרי שלוחצים על OK

