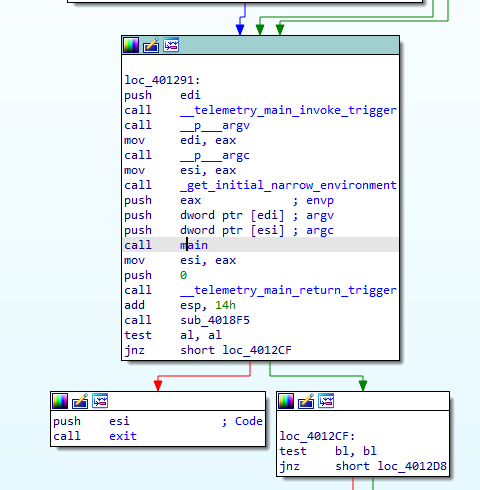
פתרון לVegas רז אברג'ל:

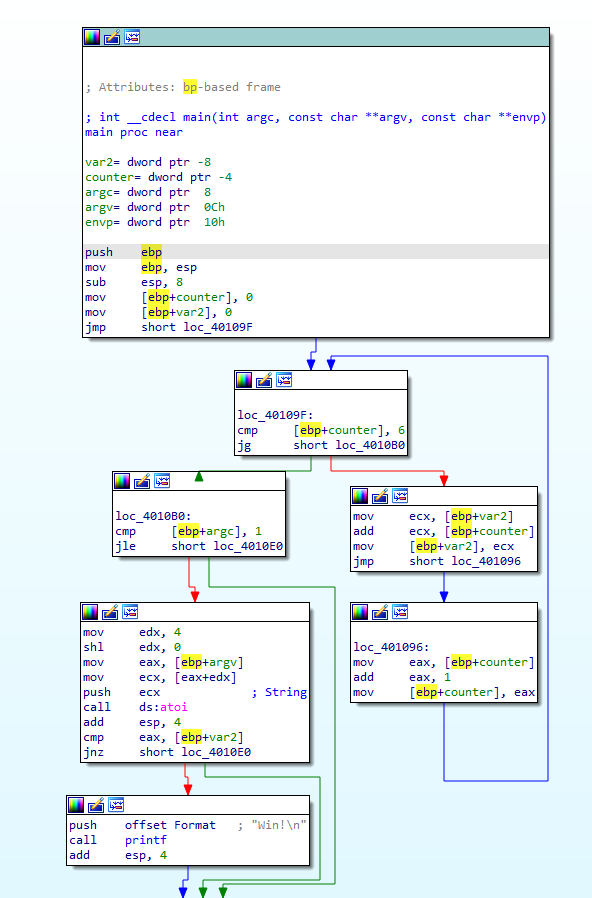
\*תחילה נמצא את הפונקציה הראשית ע"י זיהוי של שליחת ARGV,ARGC לפני קריאה לפונקציה,

והאזור שבו נחפש את הפונקציה יהיה לפני הקריאה לexit



1.לאילו פונקציות הפונקציה הראשית קוראת ? מה הכתובות שלהם ומה הפרמטרים שהן מקבלות?

תחילה נתבונן במיין



למעשה במיין יש לנו קריאה לפונקציה אחת בלבד והיא הפונקציה ATOI פונקציה זו מקבלת מחרוזת ומחזירה את הערך המספרי שלה לתוך INT

הפונקציה נמצאת בכתובת 

והפרמטר שהפונקציה מקבלת הוא המחרוזת שהוכנסה לרגיסטר ecx , מחרוזת זאת הגיעה למעשה מהפרמטר

Argv שהוא מערך של מחרוזות שמחזיק באינדקס 0 את שם הקובץ והחל מאינקדס 1 והלאה הוא מחזיק את המחרוזות שמיין יכולה לקבל .

2.איך ננצח את המשחק ?

במיין יש לנו שתי משתנים לוקלים הראשון - counter הוא מונה לולאה שרצה שמונה פעמים.

השני VAR2 שהולך ומוסיף על עצמו כל איטרציה את המשתנה הראשון כך שביציאה מהלולאה הוא מקבל את הערך 21.

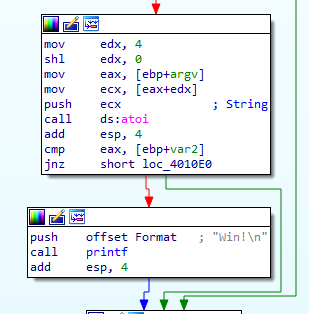
ברגע שהלולאה הסתיימה נגיע לחלק השמאלי בתרשים לכתובת 

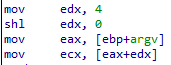
שם יהיה לנו תנאי שיבדוק אם המשתנה המקומי argc (שהוא למעשה מונה את מספר הארגומנטים שמיין מקבלת) קטן או שווה ל1 אם הוא קטן או שווה לאחד (זה אומר בעצם שהמיין לא מקבלת פרמטרים בכלל למעט שם הקובץ ) אם אכן לא שלחנו פרמטרים באותה שורה של שם הקובץ אנחנו נקפוץ ליציאה מהפונקציה ואז לא יקרה כלום



מכאן שאנחנו מבינים שכדי לנצח את וגאס נצטרך לשלוח ארגומנטים (מחרוזות) למיין כדי שהתנאי לא יתקיים והקפיצה תגיע

לחלק הזה



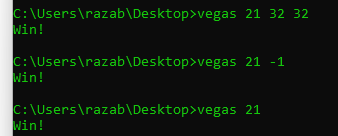
בשלב זה אנחנו רואים שאנחנו ניגשים לאיבר השני של המערך ARGV ע"י (נתקדם בארבע בתים מargv). שזה אינדקס [1] של המערך שהוא הארגומנט הראשון שנשלח בהפעלת התוכנית

המחרוזת הראשונה הנ"ל בargv היא זאת שתכנס בתור פרמטר לפונקציה ATOI וממנה יחזור בתור מספר שלם ערכה לתוך רגיסטר EAX

לאחר מכן נגיע להשוואה בין הערך שהחזירה ATOI לבין המשתנה הלוקלי השני VAR2 .

על מנת שנגיע לפונקציית ההדפסה נהיה חייבים שהשוואה בין האיבר השני של ARGV וערכו של VAR2 יהיו שווים,אם הם לא שווים דגל האפס ישאר כבוי ואז נדלג על פונקציית ההדפסה כמתואר בתרשים.

מכאן שכדי לנצח את VEGAS נפעיל את התוכנית עם שליחה של פרמטר נוסף למיין בשורת האתחול (חוץ משם התוכנית) עם הערך 21 כך שהוא יהיה שווה לערכו של VAR2 (אפשר לשלוח פרמטרים נוספים אבל זה לא ישנה את העובדה שזה יעבוד כל עוד נשלח בפרמטר הראשון את 21.



ונצחנו את VEGAS