

אלעד פישר 213924624

(1) המיין קורא ל2 פונקציות:

atoi:

הפונקציה אטוי למעשה ממירה מחרזת למספר, היא מקבלת מחרוזת כמו שניתן לראות

```
mov     ecx, [eax+edx]
push    ecx                ; String
call    ds:atoi
```

בקוד

הכתובת שלה זה: 00402048 כמו שניתן לראות בקוד:

```
.idata:00402048 ;
.idata:00402048 ; int (__cdecl *atoi)(const char *String)
.idata:00402048 extrn atoi:dword ; CODE XREF: main+45↑p
.idata:00402048 ; DATA XREF: main+45↑r ...
```

הפונקציה השניה: printf:

פרינטפ מדפיסה את המחרוזת הראשונה(פורמט) עם הפרמטרים שאחרי, זו פונקציית מערכת...

היא מקבלת אצלנו מחרוזת(למעשה זה הכתובת של המחרוזת) כמו שניתן לראות כאן

```
push    offset Format      ; "Win!\n"
call    printf
add     esp, 4
```

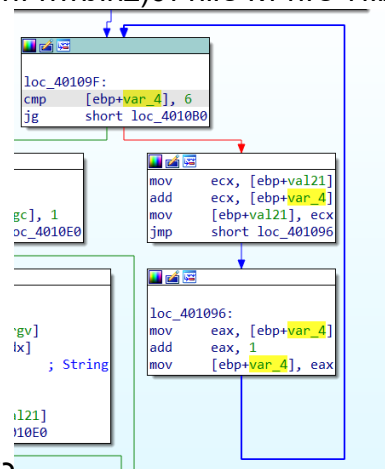
כמו כן הכתובת שלה זה 00401040 כמו שאפשר לראות בקוד

```
.text:00401040 Format
               = dword ptr 8
.text:00401040 arg_4
               = byte ptr 0Ch
.text:00401040
push    ebp
```

```
loc_40109F:
cmp     [ebp+var_4], 6
jg      short loc_4010B0
```

(2)הקוד בהתחלה בודק אם משתנה 4_שווה 6:

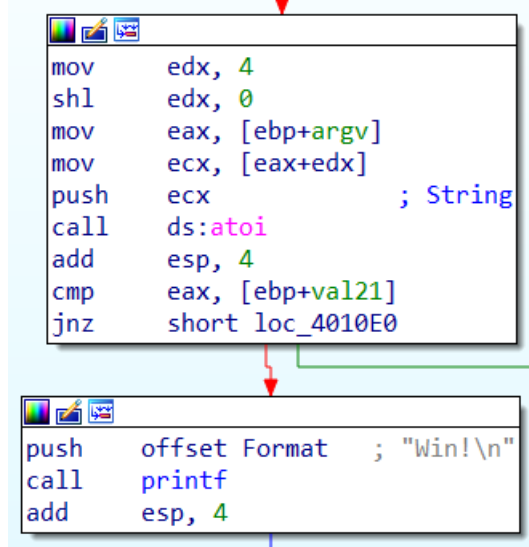
בגלל שזה לא שווה ל6(בהתחלה זה מאותחל ל0) קופצים ללולאה:



כאן אפשר לראות שכל איטרציה אנחנו נוסף

למשתנה 21 את הערך של הקאונטר(משתנה 4_) שלנו. בחלק השני אנחנו נוסף 1 לערך של משתנה 4. ושוב נבדוק את התנאי אם משתנה 4_ שווה 6.

למעשה לפי זה הלולאה תעבוד 6 פעמים ותחבר למשתנה 21_1,2,3,4,5,6 ולכן הערך שלו יהיה בצורה מפתיעה מאוד – 21. לאחר מכן שהאיטרציה תהיה שווה 6 נמשיך לקטע קוד



הבא:

כאן אנחנו נמיר את הקלט מהמשתמש בעזרת הפונקציה atoi. ונבדוק אם הערך שווה לערך של משתנה 21_. אם הערכים שווים אנחנו נקפוץ לחלק שמדפיס את הטקסט WIN! ולכן אנחנו נרצה להכניס בקלט 21 כי אז יודפס win! סתם דוגמה להרצה:

```

c:\assembly>vegas 21
Win!

c:\assembly>
  
```