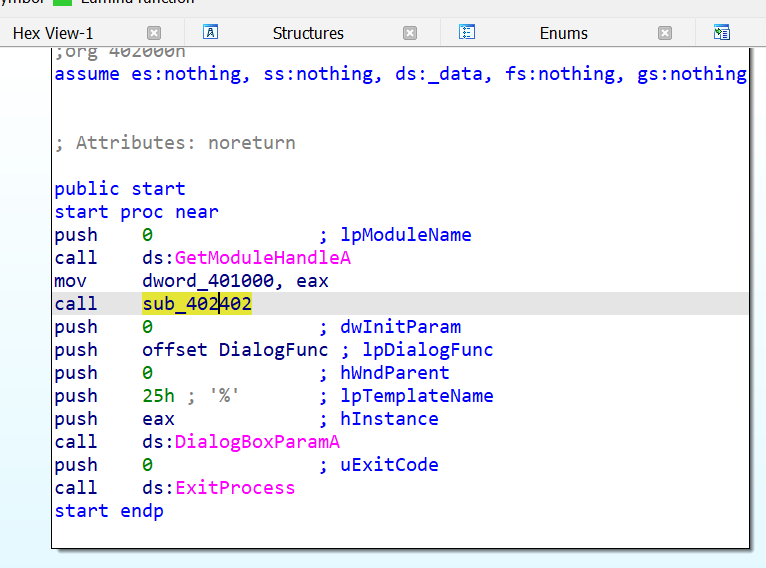
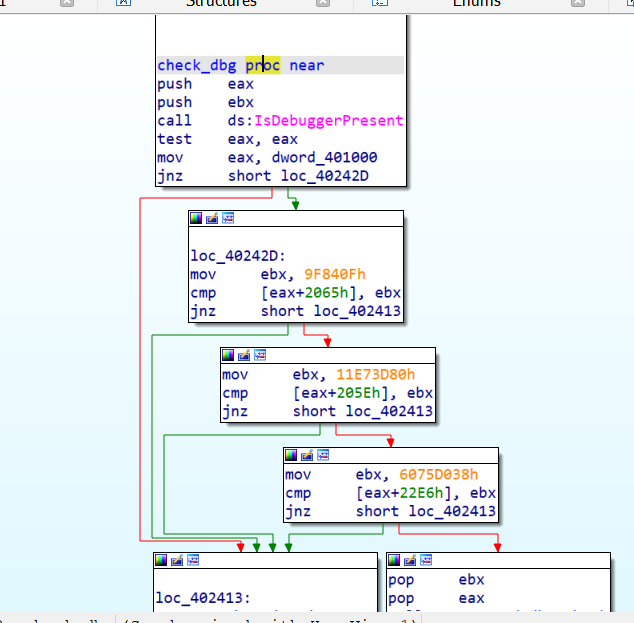
# תרגיל 9 BispooKeygen1 – נדב צימרמן

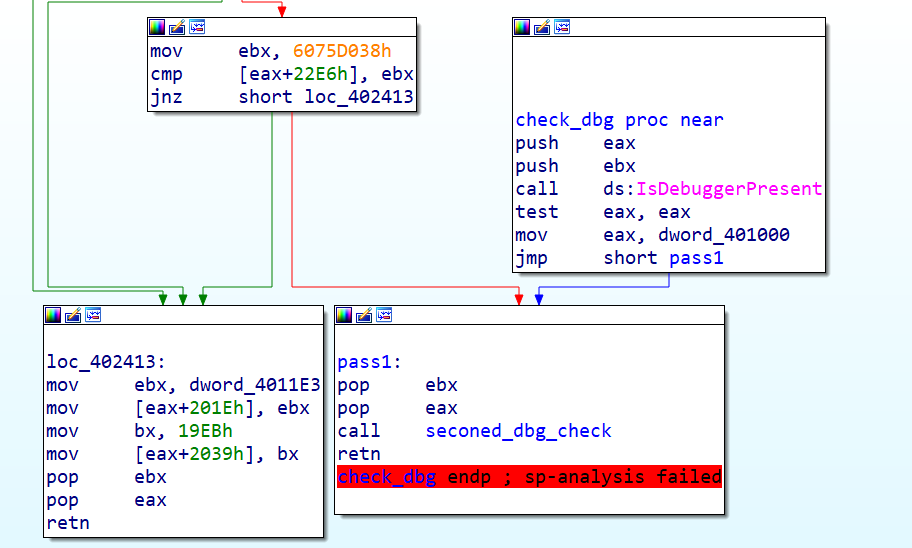
פתחתי את הקובץ בIDA על מנת להתחיל ולהבין כיצד לפרוץ אותו. בתמונה ניתן לראות את מהלך התוכנית:



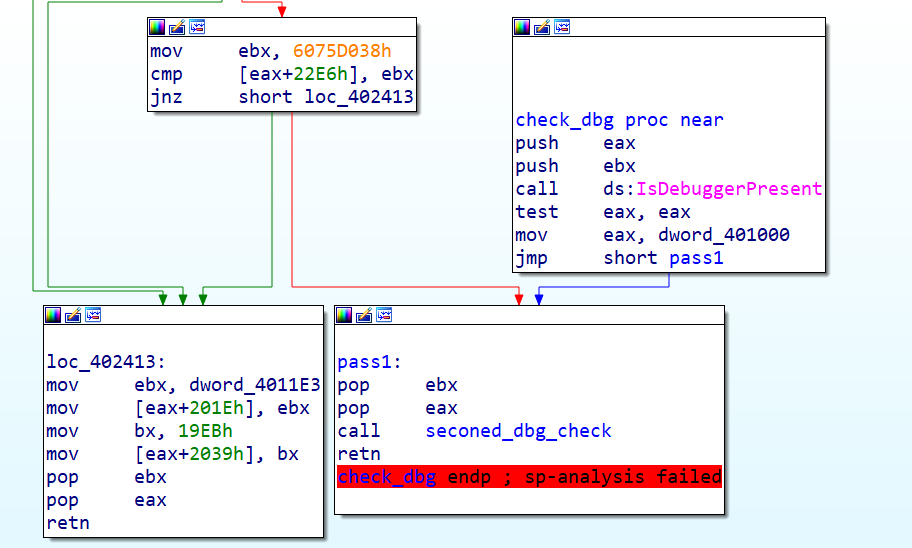
ניתן היה לראות שהפונקציה הנקראת בחלק המסומן בצהוב בודקת שהתהלך איננו מדובג בשתי בדיקות, כאשר כשל בכל אחת מהבדיקות מאפס את התוכנית.

בדיקת אנטידיבאג 1 נעשתה בפונקציה שקראתי לה check\_dbg. היא ביצעה קריאה לפונקציה IsDebbugerPresent שהחזירה 1 אם התרחש דיבוג של הקוד בזמן הבדיקה. לכן הוספתי patch שעוקף את הבדיקה כפי שניתן לראות בתמונה הבאה:

הסבר ה-patch: שיניתי את המקום המודגש JMP pass1 במקום jz, כך בכל מקרה הפונ' תדלג על הבדיקה

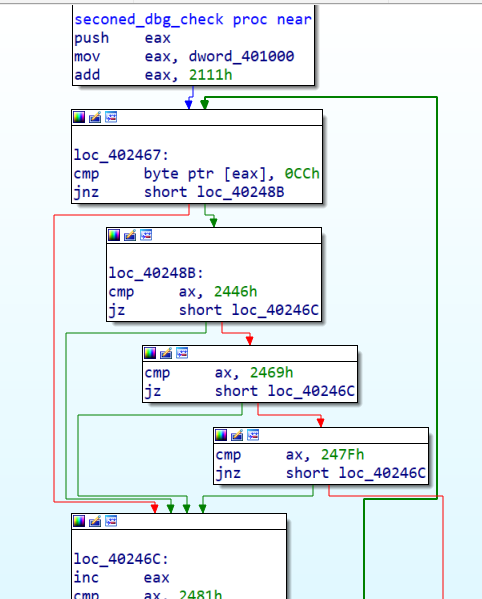
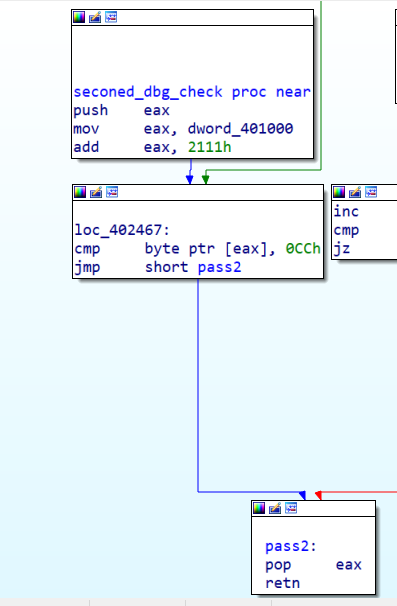


הקריאה לבדיקה שנייה (נקראת ע"י פונקציית הבדיקה הראשונה) :



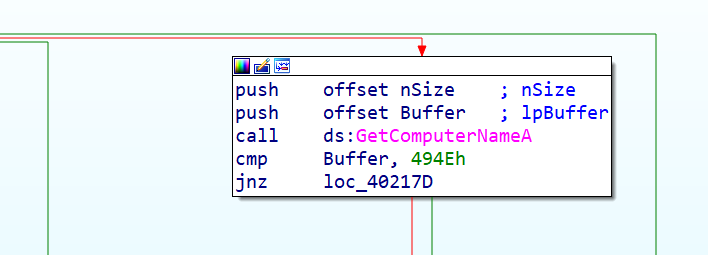
בדיקה 2 מבצעת מעבר על הקוד ומחפשת שורות שמתחילות בתו 'CC'. כפי שהסברנו בהרצאה כל ברייקט פוינט בשורה מחליף את הבייט הראשון בשורה בתו זה. על מנת לדלג על הבדיקה פשוט דילגתי על כל הבדיקה הזו כפי שניתן לראות להלן:

הpatch בבדיקה השנייה – jmp במקום jz כך שגם אם קיים breakpoint הבדיקה תעבור לסוף פונקציית הבדיקה:

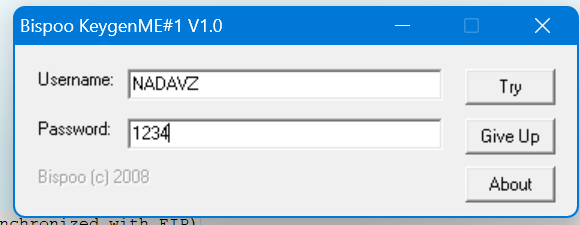


לאחר מכן חזרתי לקוד הראשי (כפי שניתן לראות בתמונה הראשונה במסמך זה), לפי המבנה של הפונקציה DialogBoxParamA שניתן למצוא בגוגל ובתרגילים קודמים הפונקציה מקבלת פונקציה (dialogfunc) והגדרות נוספות לחלון שייפתח במהלך התוכנית, לכן עברתי לבדוק את dialogfunc לאחר שטיפלנו בבדיקות הדיבוג.

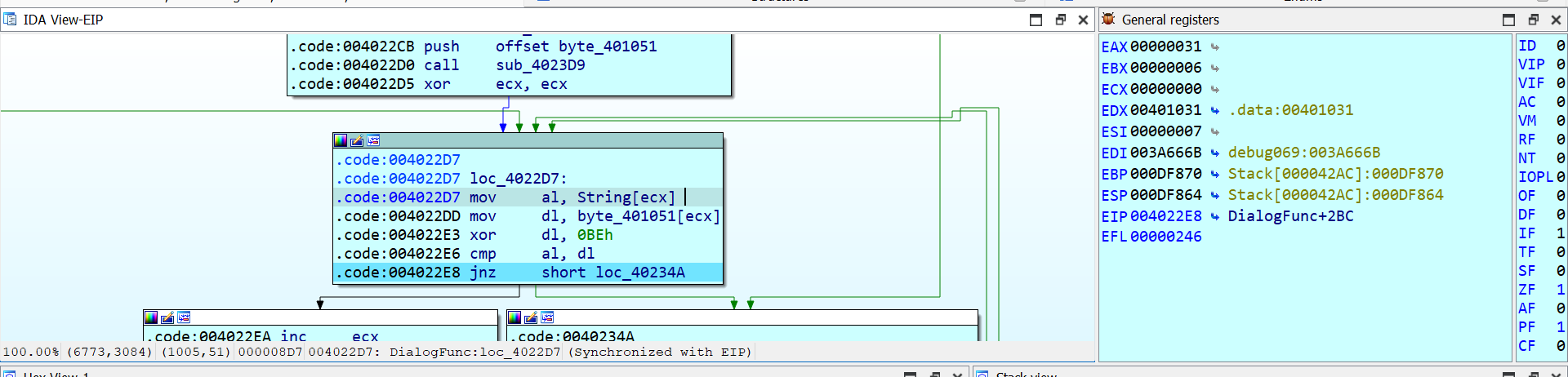
חיפשתי פרטים שיירמזו לי על שמות המשתמשים האפשריים וראיתי שיש קריאה לפונקציה GetComputerNameA של ווינדווס.



משיטוט קצר ( ושם הפונקציה עצמה) הבנתי שהיא מחזירה את שם המחשב, הנחתי שמדובר בשם המשתמש שצריך להכניס בתיבה שנמצאת בהרצה. ניסיתי להכניס זאת בדיבוג במהלך ההרצה וראיתי כי קיבלתי שהסיסמא שגויה:

תמונה שמכילה טקסט, גופן, מספר, תוכנה

התיאור נוצר באופן אוטומטי

חזרתי ודיבגתי לעומק את הפונקציה dialogfunc, וראיתי שבמהלך הפונקציה התוכנית עוברת תו אחר תו בסיסמה שהוכנסה, ומשווה את קוד האסקי של התו למספר שמופיע לאחר xor עם המספר ההקסדצימלי Beh. כפי שניתן לראות להלן:

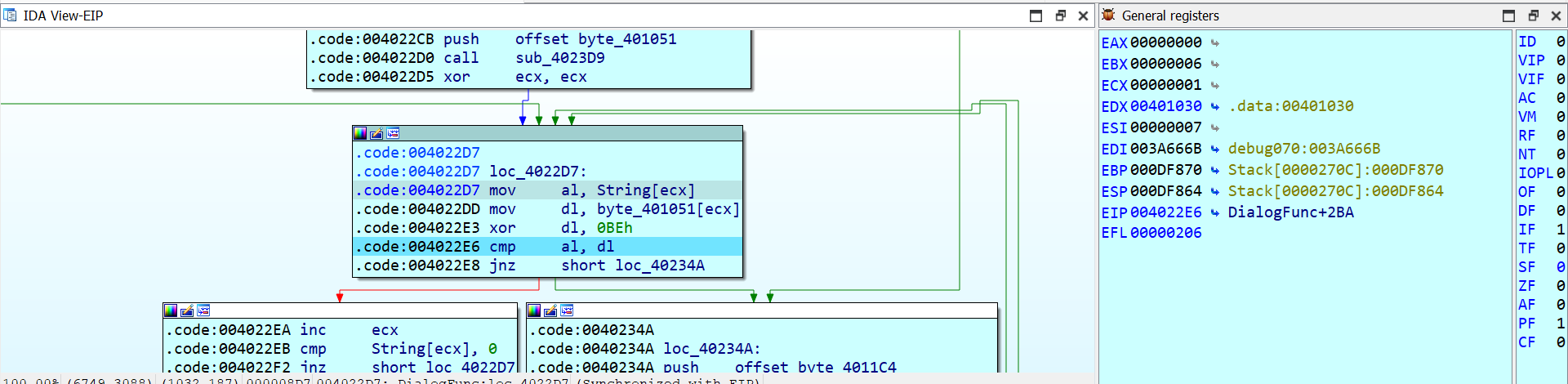
הסבר לתמונה: ברגיסטר al מופיע האסקי של התו שנבדק (31 – '1' בדוגמה) והוא מושווה לתו בזיכרון התוכנית לאחר הxor (גם 31 – '1' בתו הראשון בסיסמא), כך הבנתי שהתו הראשון צריך להיות 1.

המשכתי כך תו אחר תו עד לקבלת הסיסמא הרצויה.

דוגמה למציאת התו הבא בסיסמא (0) לאחר 1:

תמונה שמכילה טקסט, צילום מסך, גופן, מספר

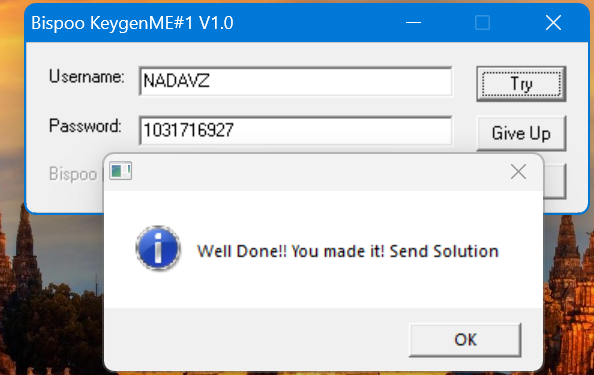
התיאור נוצר באופן אוטומטיהקלט שהכנסתי:

ניתן לראות בתמונה להלן (לאחר ההשוואה של התו הראשון – 31 באסקי), כי ברגיסטר al יש 00 משום שהכנסתי סיסמא בעלת התו '1' בלבד, והתוכנית השוותה זאת לרגיסטר dl בו היה 30, הקידוד האסקי של התו '0'.

חזרתי על הפעולה שתוארה בסעיף האחרון וראיתי כי הסיסמא המתקבלת היא 1031716927, הרצתי זאת וקיבלתי את הודעת ההצלחה הבאה:

תמונה שמכילה טקסט, צילום מסך, גופן, מספר

התיאור נוצר באופן אוטומטי



**סיסמאות נוספות:**

|  |  |
| --- | --- |
| שם משתמש | סיסמא |
| 62019976755 | MYMAN |
| 2133195254 | ABCD |
| 61221775831 | ME23 |
| 61979765627 | aaaa |