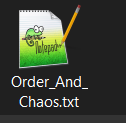
# פיתרון CTF2

* ניתן לראות כי קיימים 300 קבצים בתיקייה הראשית שאם נסתכל בכל אחד מהם באמצעות notepad

נמצא רצף תווים שונה. לדוגמא -

* 
* אם נחבר את תוכן הקבצים הללו לקובץ אחד, נקבל קובץ חדש ותקין. על מנת לעשות זאת נאלץ למצוא את הסדר הנכון להרכבת הקובץ.
* אם נתבונן בקובץ OrderAndChaos נמצא שם סטרינג ארוך המקודד בbase-64.

NjksMjg3LDU1LDI0OCwyMzUsNDMsMTg0LDIsMjgzLDEzNCwyMTYsMTUsMjk0LDUyLDUzLDgzLDE4

NiwyNzIsMTI4LDM5LDEsMjgsMjk2LDEzNSwxMzYsMyw0LDIyMCwxMzEsMTcwLDE3MiwyNTEsMjA5

LDIyNiwyNTAsMTQzLDI2OCw1LDE5Niw2LDE5LDExMSwxNywxMywyMTQsNywxNDcsOTksNDEsMjc0

LDE5MCwyNzUsOCwyMzcsMTYxLDE4OSw3MiwyMTIsMTA4LDI1NCwxMzMsMzEsMjU3LDksMjU2LDIw

NiwxMCwyNzYsOTEsMTEsMjc4LDE2MiwyOTMsMTIsMTc0LDI1OSwxMTQsMjAsNTcsMTQsNDYsMjk4

LDIzMiwxNiwyMzQsOTIsMTgsMjEsMjIsOTMsMjMsMjQsMTIzLDI1LDIyOCwyNiwyNywxNjMsMTA2

LDExOSw0NSwyOSwyODAsMzcsMzAsMjA1LDQ3LDI0MSwyMjQsMTA0LDE5OSwyNjksMTUzLDEzMCw2

Nyw4NywyMjIsMzIsMTk1LDMzLDE5NywzNCwzNSw3MSwzNiwzOCwyMDEsNDAsMjUzLDU4LDEyMSw0

OSwxOTIsMTAwLDEzNyw0Miw0NCw0OCw1MCwyNzksNTEsMjYyLDMwMCwxOTEsNTQsMTE4LDU2LDU5

LDE2OSw2MCwyODgsMTE3LDE4MCwxNTAsMTg4LDIwNywyNDAsMTQwLDYxLDI0NCwxOTgsNjIsNjMs

MTQxLDY0LDE4MSw2NSw2Niw2OCw3MCwyMTMsMTU0LDIzNiwyNjQsNzMsNzQsODEsMTI1LDkwLDc1

LDc2LDEyOSw3Nyw3OCw3OSw4MCwxODUsMjcwLDE0NSw4MiwyNjUsOTQsMTczLDg0LDI4Niw4NSw4

Niw4OCw4OSw5NSwyMjMsOTYsOTcsMTU4LDk4LDEwMSwxMDIsMjk1LDEwMywxMDUsMTA3LDIyNywx

MDksMTEzLDExMCwxODIsMTEyLDE0MiwyMDMsMTE1LDExNiwxMjAsMTU5LDEyMiwxMjQsMTQ0LDIx

MSwxMjYsMTI3LDEzMiwxMzgsMTM5LDE0NiwxNDgsMjI1LDE2NCwyMzgsMTYwLDIxMCwxNDksMTUx

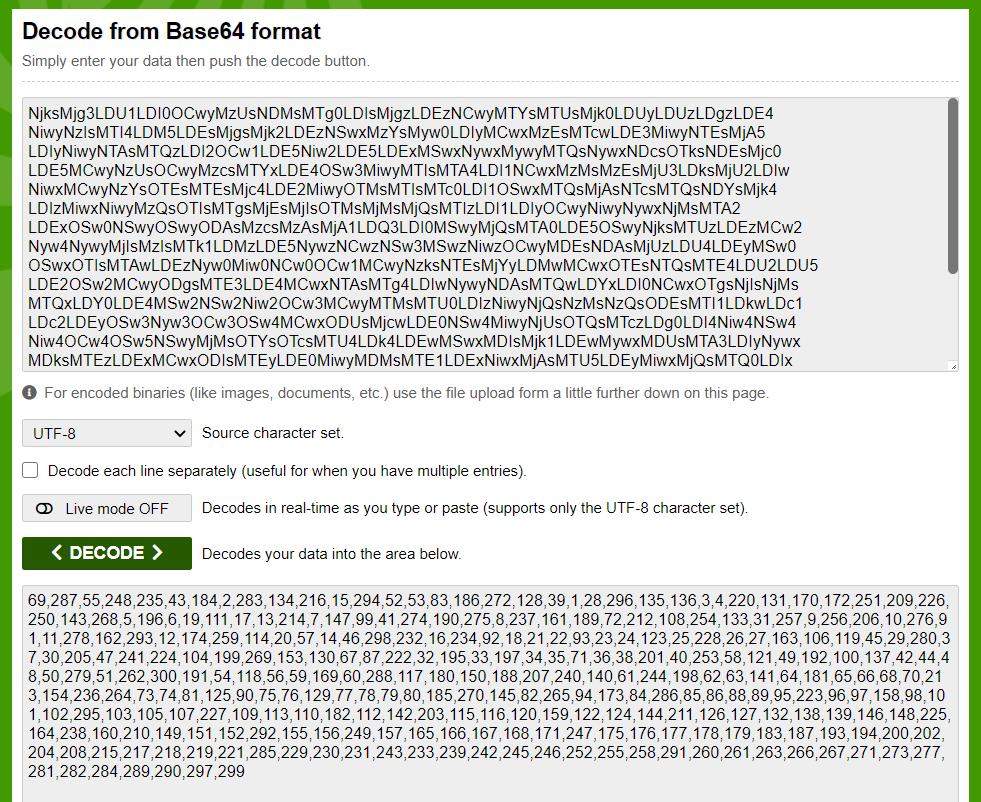
LDE1MiwyOTIsMTU1LDE1NiwyNDksMTU3LDE2NSwxNjYsMTY3LDE2OCwxNzEsMjQ3LDE3NSwxNzYs

MTc3LDE3OCwxNzksMTgzLDE4NywxOTMsMTk0LDIwMCwyMDIsMjA0LDIwOCwyMTUsMjE3LDIxOCwy

MTksMjIxLDI4NSwyMjksMjMwLDIzMSwyNDMsMjMzLDIzOSwyNDIsMjQ1LDI0NiwyNTIsMjU1LDI1

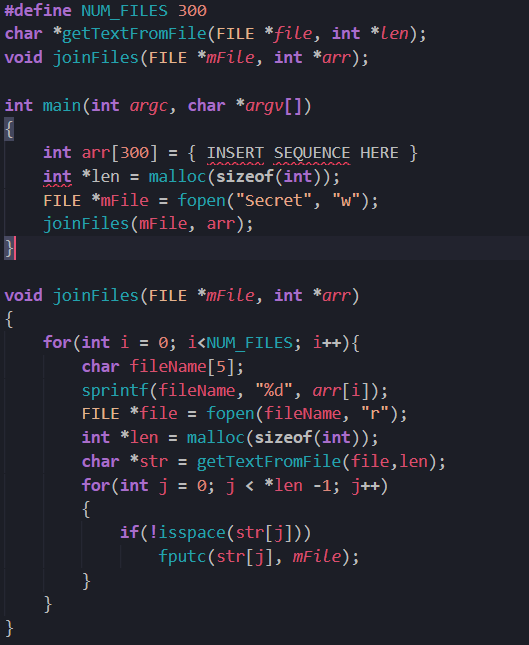
OCwyOTEsMjYwLDI2MSwyNjMsMjY2LDI2NywyNzEsMjczLDI3NywyODEsMjgyLDI4NCwyODksMjkw

LDI5NywyOTk=

*  נהפוך אותו לקוד ASCII באמצעות האתר הבא – [Base64 Decode and Encode - Online](https://www.base64decode.org/)

* ונקבל את הסדר שבו הקבצים צריכים להיות מורכבים -

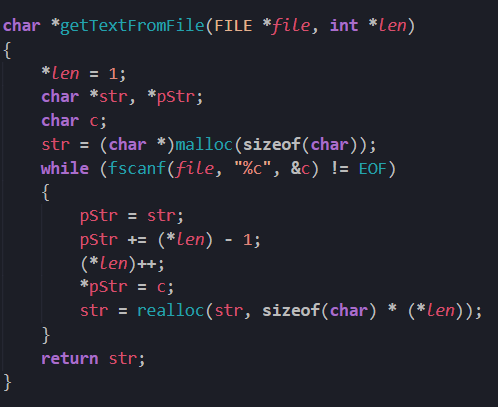
69,287,55,248,235,43,184,2,283,134,216,15,294,52,53,83,186,272,128,39,1,28,296,135,136,3,4,220,131,170,172,251,209,226,250,143,268,5,196,6,19,111,17,13,214,7,147,99,41,274,190,275,8,237,161,189,72,212,108,254,133,31,257,9,256,206,10,276,91,11,278,162,293,12,174,259,114,20,57,14,46,298,232,16,234,92,18,21,22,93,23,24,123,25,228,26,27,163,106,119,45,29,280,37,30,205,47,241,224,104,199,269,153,130,67,87,222,32,195,33,197,34,35,71,36,38,201,40,253,58,121,49,192,100,137,42,44,48,50,279,51,262,300,191,54,118,56,59,169,60,288,117,180,150,188,207,240,140,61,244,198,62,63,141,64,181,65,66,68,70,213,154,236,264,73,74,81,125,90,75,76,129,77,78,79,80,185,270,145,82,265,94,173,84,286,85,86,88,89,95,223,96,97,158,98,101,102,295,103,105,107,227,109,113,110,182,112,142,203,115,116,120,159,122,124,144,211,126,127,132,138,139,146,148,225,164,238,160,210,149,151,152,292,155,156,249,157,165,166,167,168,171,247,175,176,177,178,179,183,187,193,194,200,202,204,208,215,217,218,219,221,285,229,230,231,243,233,239,242,245,246,252,255,258,291,260,261,263,266,267,271,273,277,281,282,284,289,290,297,299

* נבנה תוכנית בסיסית העוברת על הקבצים לפי הסדר שמצאנו ונחבר אותם לקובץ אחד.
* את התוכנית נכתוב בשפת C.

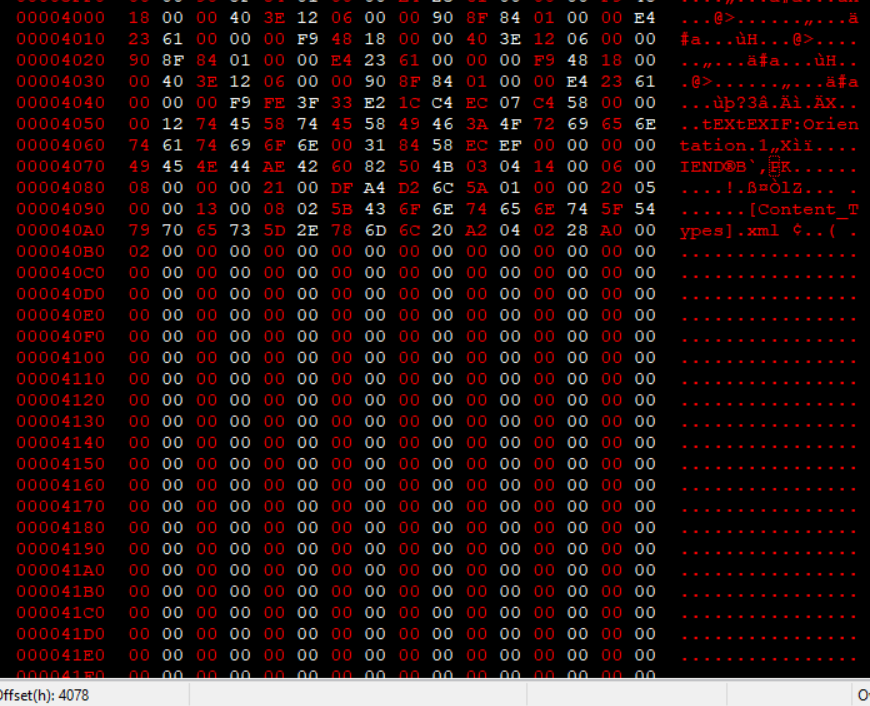
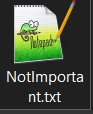
התוכנית מייצרת קובץ חדש בשם secret, וקוראת לפונקציה joinfiles.

כמו כן סדר התווים של ההרכבה יכנס למערך בגודל 300 כפי שקיבלנו אותו.

הפונקציה מקבלת קובץ ומערך של מספרים, קוראת את הקבצים אחד אחד לפי הסדר של ההרכבה במערך שקיבלה, ומעתיקה אותם לקובץ החדש שלנו SECRET.

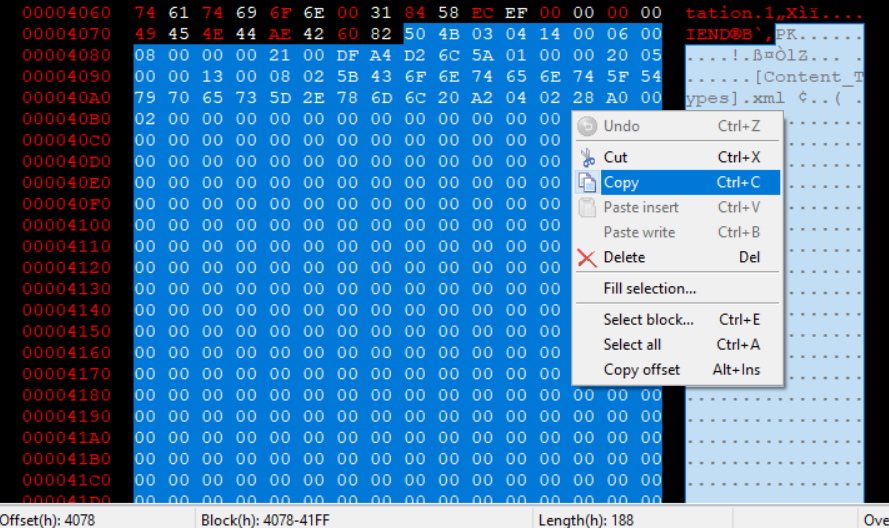


את הקריאה של טקסט מקובץ תבצע באמצעות הפונקציה הזאת שעוברת תו תו ומכניסה אותם למערך שיוחזר לפונקציה הקוראת.

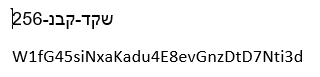
* כעת לאחר שסיימנו לכתוב את התוכנית נשמור אותה בשם joiner.c ונקמפל.
* נריץ את קובץ ההרצה החדש שלנו –
* נקבל קובץ חדש בשם Secret שאת תוכנו אנו לא יודעים!
* הקובץ החדש הינו קובץ מוצפן! נוכל לקבל רמז לכך בהתבוננות על התפוח אדמה המצורף כתמונה.
* נפתח את התמונה Cute.jpg באמצעות Hex editor .
* נראה כי התמונה שלנו נגמרת בדיוק ב4078 לפי סימן ה-IEND.
* כמו כן ניתן לקבל אישוש להימצאותו של קובץ בהיסט הזה בדיוק באמצעות קובץ רמז בשם notimportant הנמצא בתיקיה של האתגר, ומכיל את ההיסט של הקובץ המוסתר.



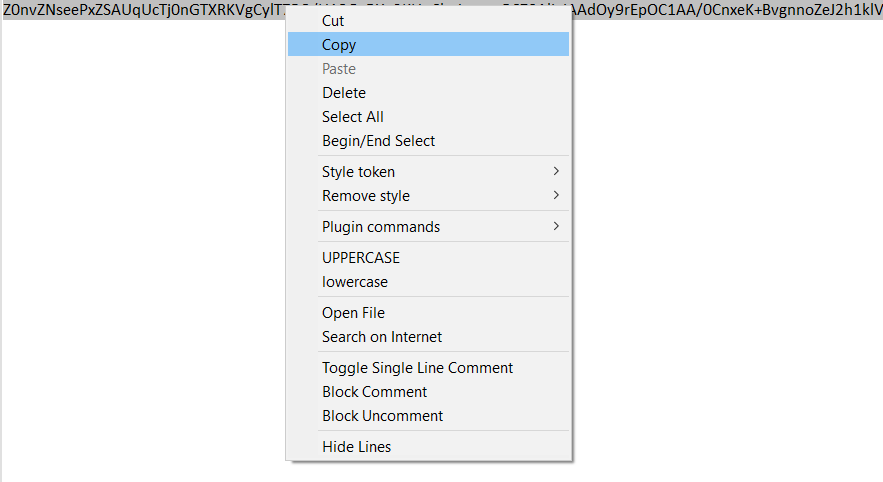
* נעתיק את הקובץ החבוי מתחילתו עד סופו –



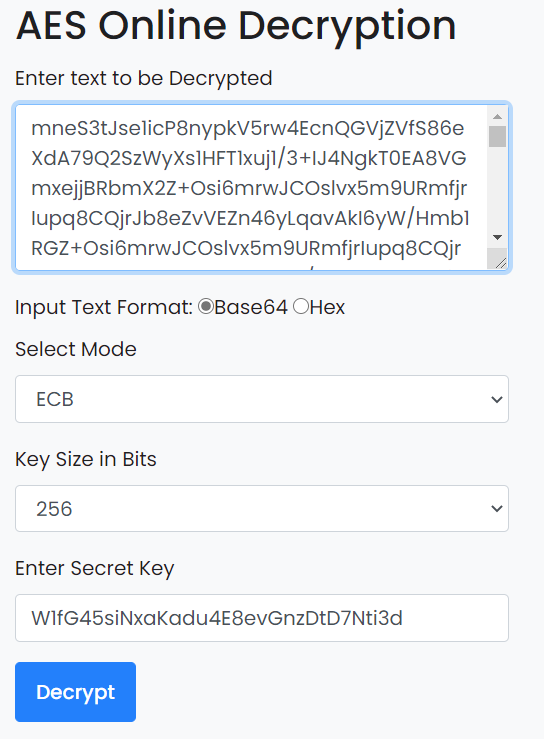
נדביק בקובץ חדש ונשמור בשם something.docx. מדוע docx? כיוון שאנו רואים כי הקובץ מתחיל ב –  
 50 4B 03 04 שזהו ה-magic number של קבצי וורד.

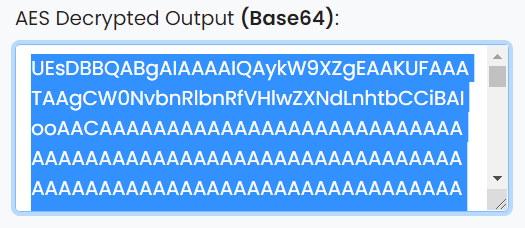
* נפתח את הקובץ שמצאנו ונקבל קובץ WORD ובתוכו מפתח ושיטת ההצפנה שכתובה באותיות בעברית.. AES – ECB – 256 🡪 שקד קבנ – 256 ..
* W1fG45siNxaKadu4E8evGnzDtD7Nti3d

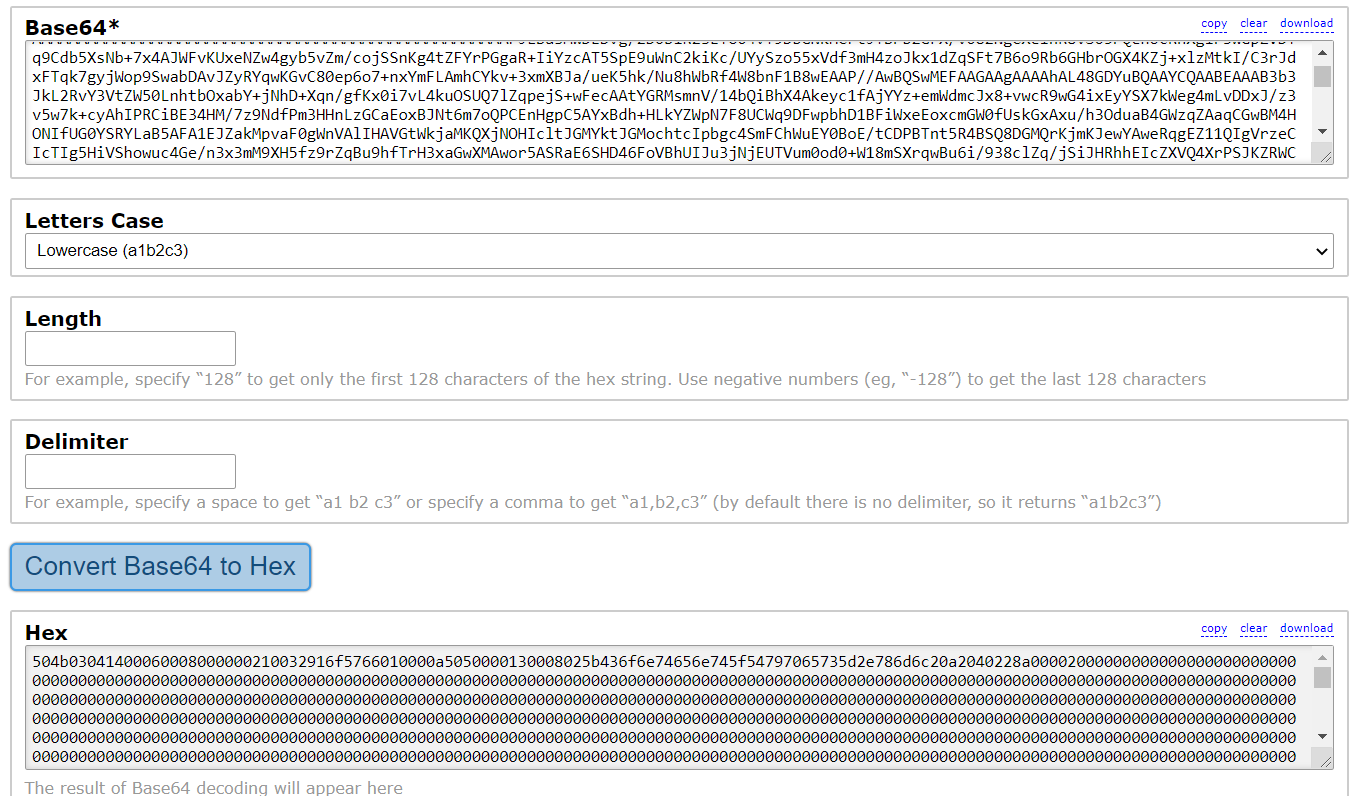
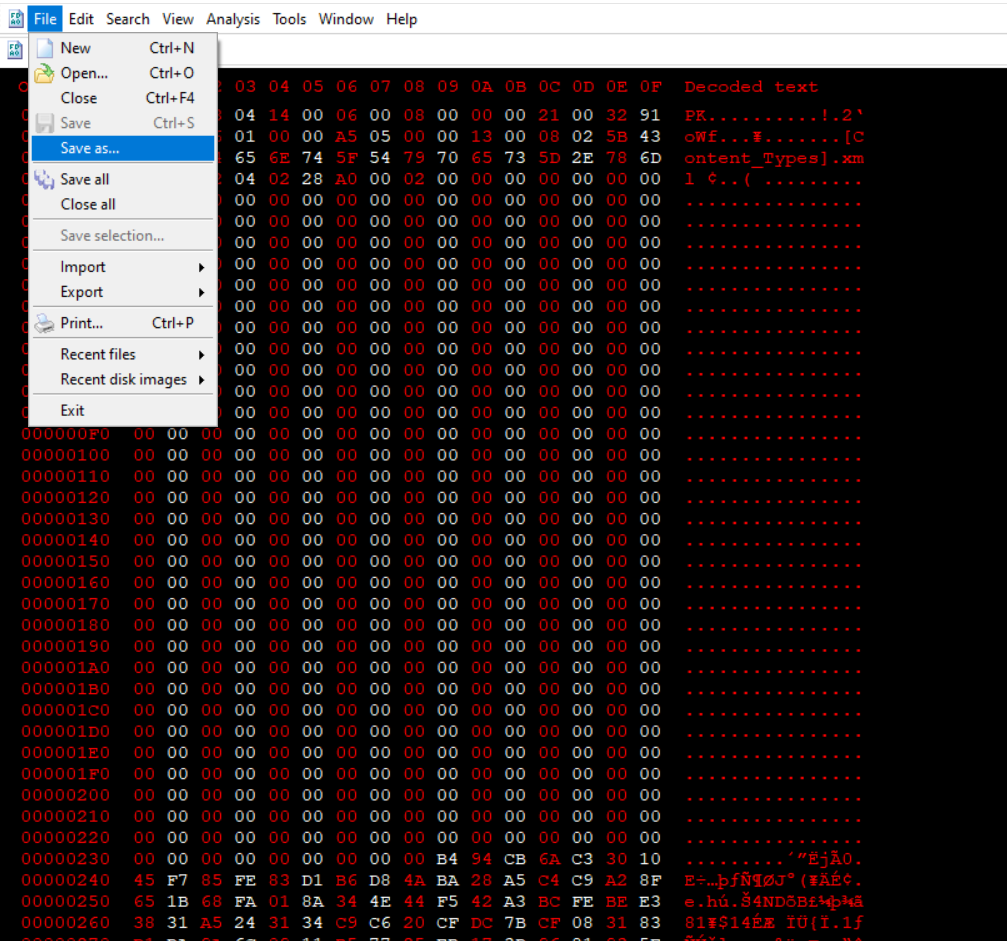
* כעת יש בידינו שיטת הצפנה, מפתח וקובץ מוצפן!
* נתחבר לאתר [Online Tool for AES Encryption and Decryption (devglan.com)](https://www.devglan.com/online-tools/aes-encryption-decryption) שיפענח לנו את הקובץ.
* נסמן שיטת ECB עם 256 ביט ונכניס את המפתח שלנו.



* האתר דורש את תוכן הקובץ ולכן נפתח את Secret שלנו באמצעות notepad ונעתיק את תוכנו.
* נדביק את תוכן הקובץ ונלחץ Decrypt.



* הפלט שהתקבל הינו בbase64.
* נעביר אותו לhex באמצעות [Base64 to Hex | Base64 Decode | Base64 Converter | Base64](https://base64.guru/converter/decode/hex)
* נדביק את התווים שלנו באתר ונלחץ Convert.
* גם כאן ניתן לראות כי הפלט שהתקבל מתחיל ב – 50 4b 03 04, ולכן זה הינו קובץ וורד.
* נשמור את הפלט כקובץ באמצעות hex editor.



* ניתן לקובץ החדש שם עם סיומת docx ונפתח אותו!
* נקבל את האפיקומן שלנו!



**Afikoman{PotatoesGun}**