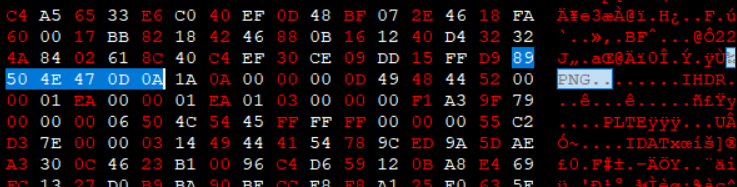
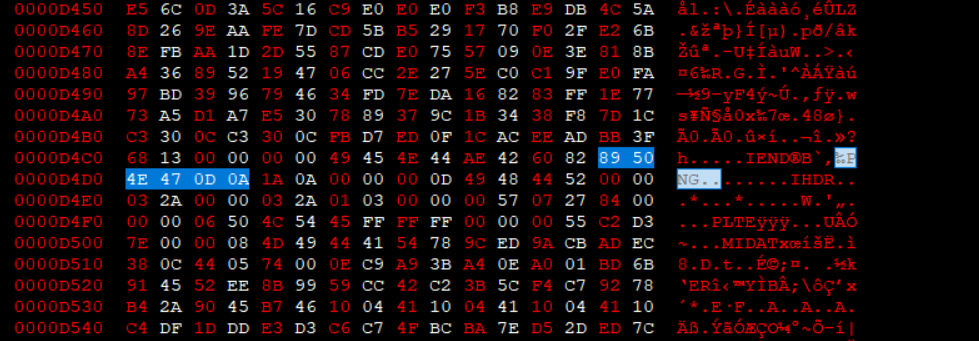
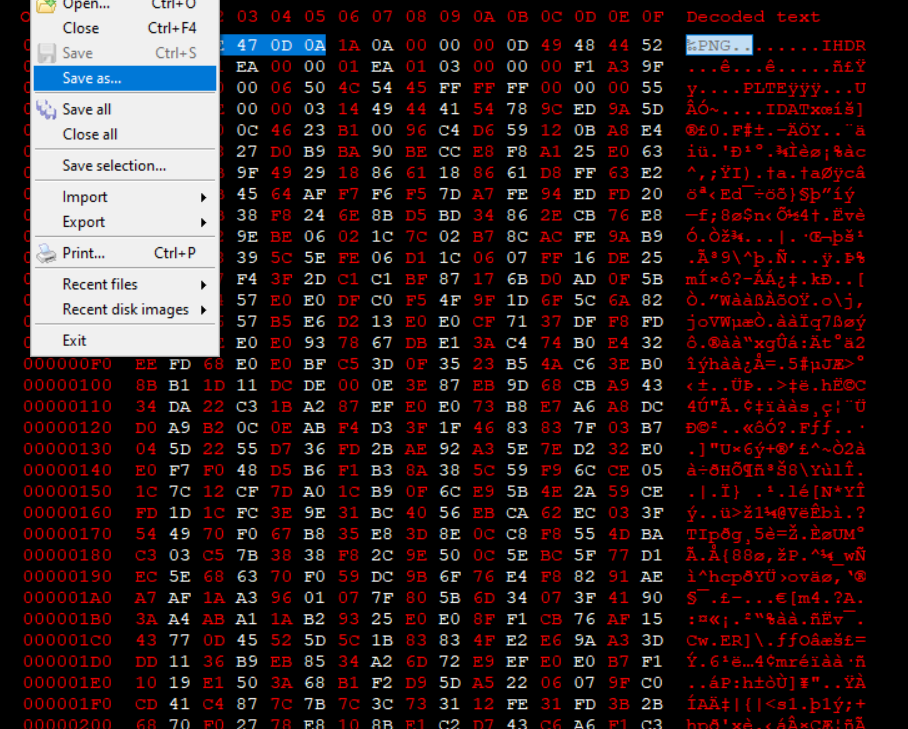
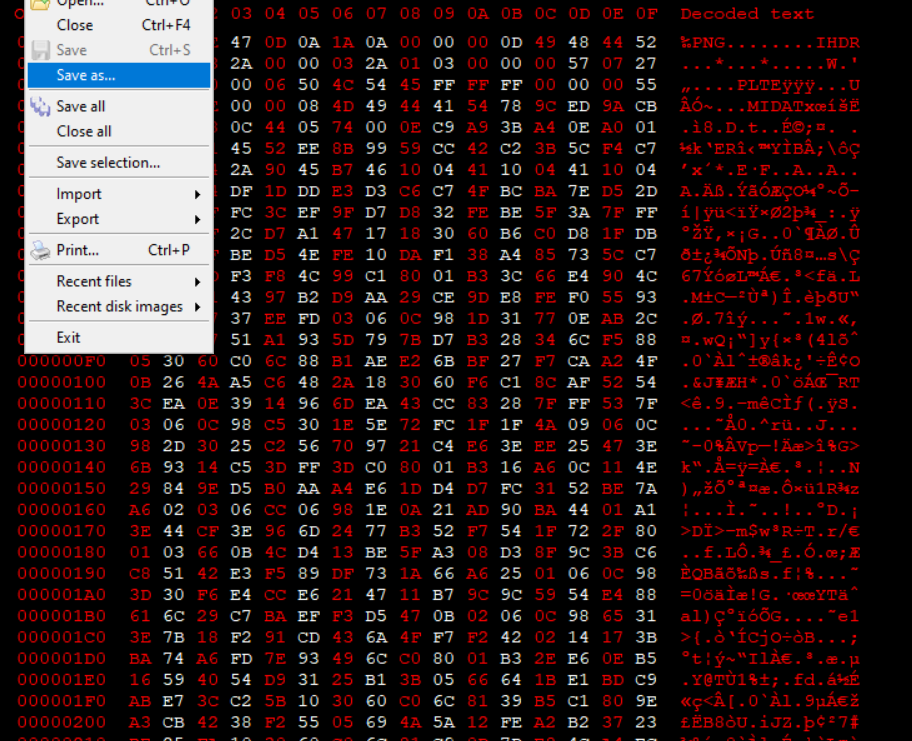
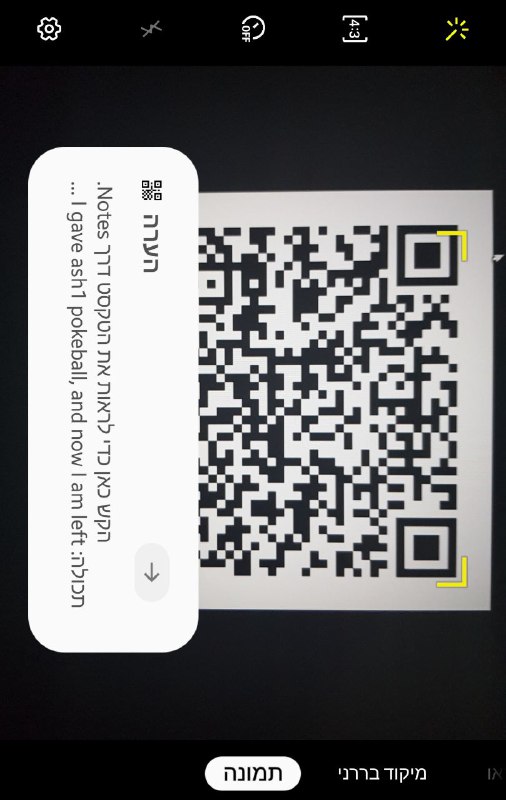
# פתרון CTF4

* בתיקית הCTF ניתן למצוא 4 תמונות וקובץ 7zip מוצפן.
* פרופסור אוק יכול לעזור לנו להבין מה אנחנו מחפשים (אחרי הכל הוא פרופסור)..
* נברר מה הוא מסתיר באמצעות hex-editor.
* ניתן לראות כי זהו magic number של קובץ מסוג PNG.
* נתבונן בהמשך הקובץ ונוכל למצוא את הרצף הזה שוב -
* קיימים כאן שני קבצים מוסתרים למעשה ושניהם קבצי PNG. נחלץ אותם על ידי העתקת הhex אל קובץ חדש ושמירה בשם.
* נדגיש את תחילת החלק הראשון עד לתחילת החלק השני ונעתיק.

נשמור את הקובץ הזה בשם PNG1.



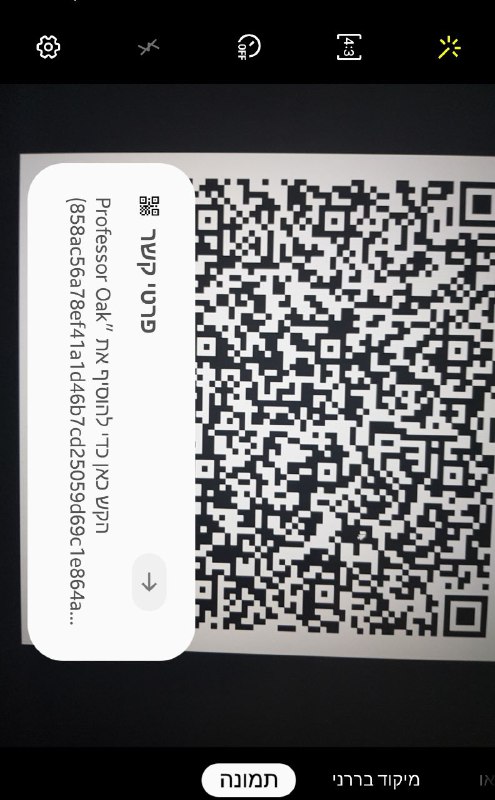
ואת השני PNG2 –

* התמונה הראשונה מכילה ברקוד המציג בפנינו לאחר סריקה קטע טקסט חשוב –

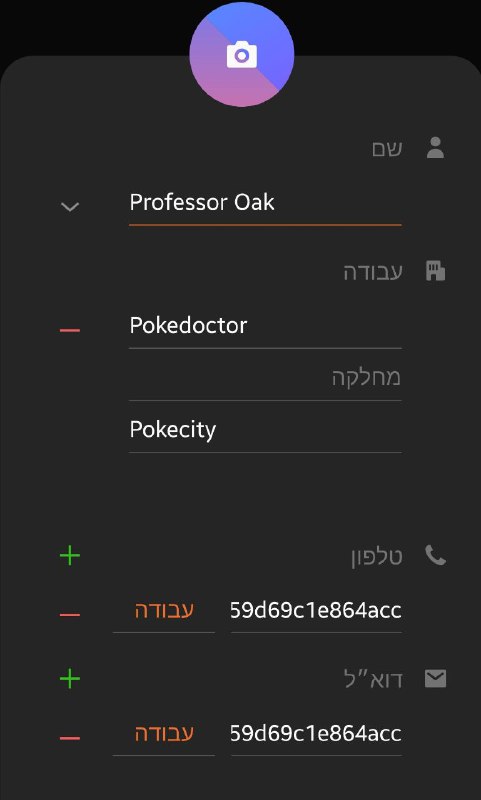
I gave ash1 pokeball, and now I am left with 1 too..

If I could get ash back, i would have caught the 2 fishes already..

קיימים כאן למעשה מספר רמזים –

הראשון הוא ash1. אש הוא דמות מפתח בפוקימון אך בנוסף לכך הוא גם פונקצית גיבוב! איזה בדיוק? ה1 הצמוד לו אמור לרמוז לנו על פונקציה מוכרת בשם sha1!  
"אם הייתי יכול לקבל את אש חזרה.." – כנראה שניתקל בקטע hash שנצטרך להחזיר את המקור שלו.  
"הייתי תופס שני דגים.." – שני דגים, באנגלית – two fish שזהו לא במקרה גם שם של הצפנה ידועה.

* התמונה השניה מכילה גם היא ברקוד אך פה אנחנו נקבל קובץ Contact של פרופסור Oak!



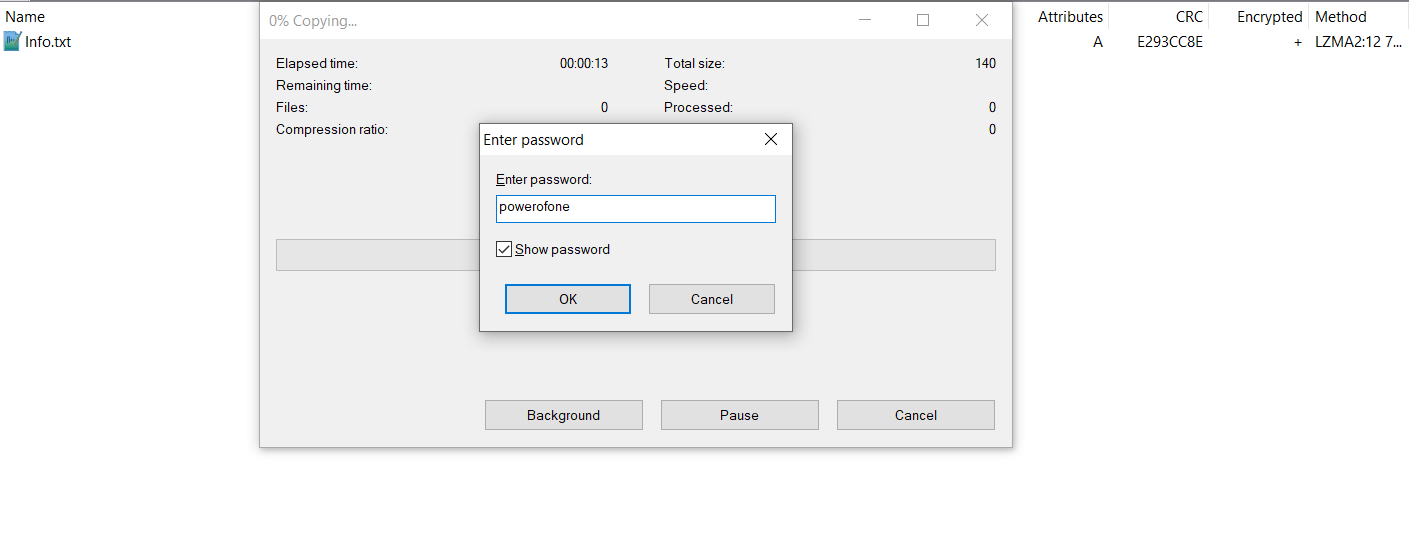
* בקובץ קיים מידע מאוד חשוב על הפרופסור כמו גם מידע פחות חשוב – סטרינג מגובב -

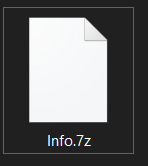
**858ac56a78ef41a1d46b7cd25059d69c1e864acc**

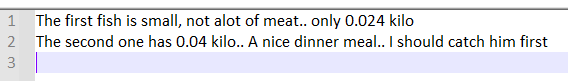
* הפרופסור אמר לנו שנצטרך להבין מה עומד מאחורי הסטרינג וזה בדיוק מה שנעשה !
* ניכנס לאתר [Sha1 Decrypt & Encrypt - More than 15.000.000.000 hashes (md5decrypt.net)](https://md5decrypt.net/en/Sha1/#answer)

****ונעתיק את קטע הסטרינג. נקבל תוצאה במיידי – **powerofone**

יצא הגורל וזהו שמו של סרט פוקימון ישן וגם כוחו של האחד (sha 1) 😊.

* כעת נתבונן בקובץ הזיפ המוצפן וננסה להכניס את מה שהרגע מצאנו -





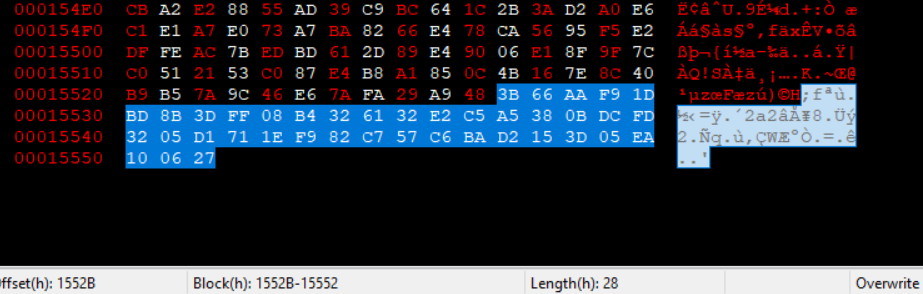
* הסיסמא אכן נכונה וכעת יש בידינו רמז נוסף!

The first fish is small, not alot of meat.. only 0.024 kilo

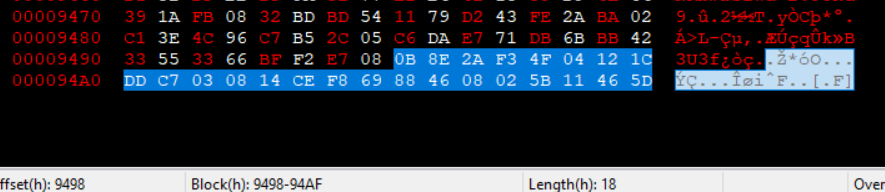
The second one has 0.04 kilo.. A nice dinner meal.. I should catch him first

קטע הטקסט הזה למעשה מכוון אותנו למידע החבוי בתוך כל אחד מהדגים.

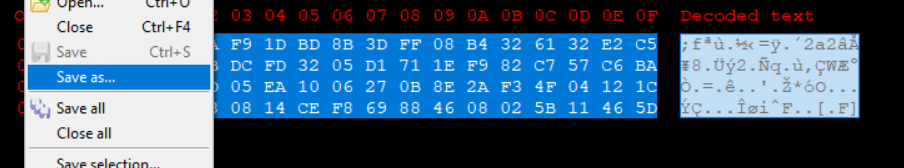
למעשה כל אחד מכיל בתוכו קטע hex רנדומלי בסופו ולכן אנו חייבים את המידע מהטקסט הנ"ל.

* ניתבונן בדג מספר 2 – ניקח את 40 הבתים האחרונים שלו ונוסיף להם את 24 הבתים האחרונים מדג מספר 1

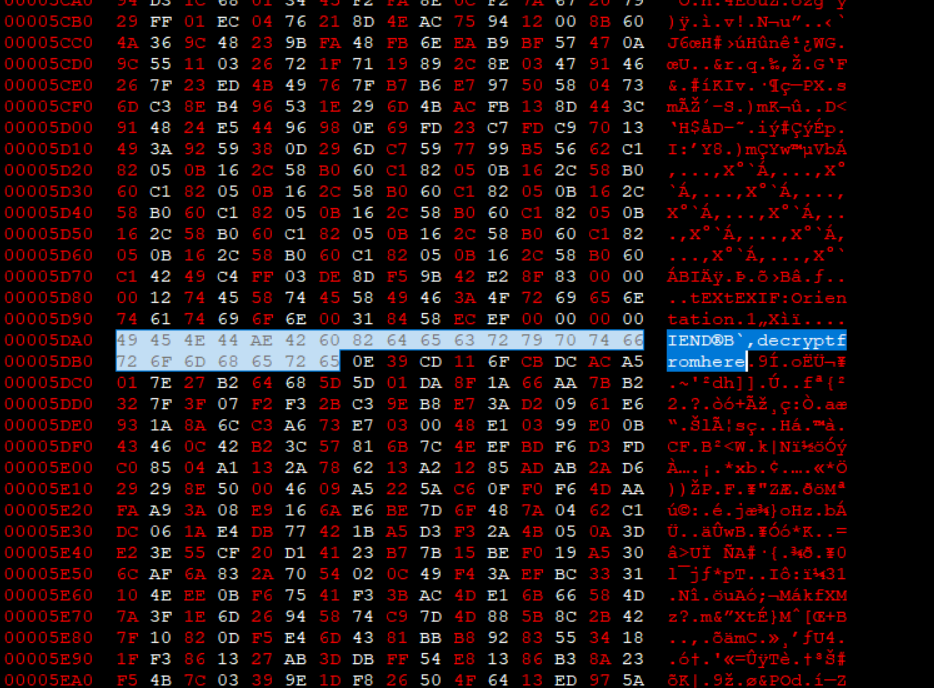
דג מספר 1-

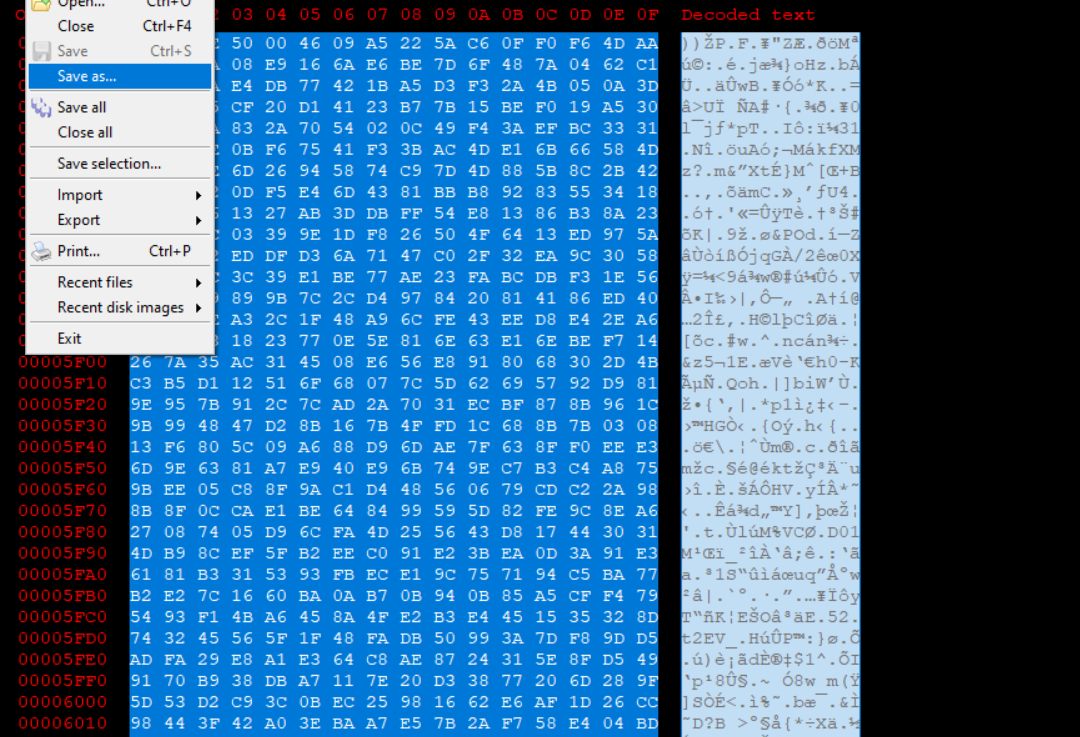


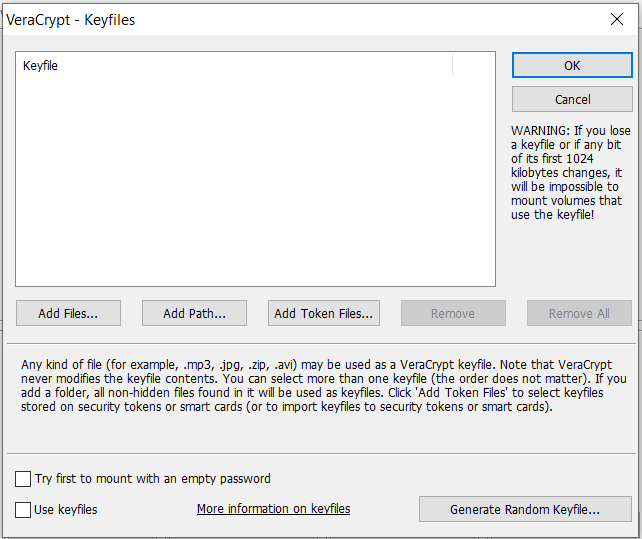
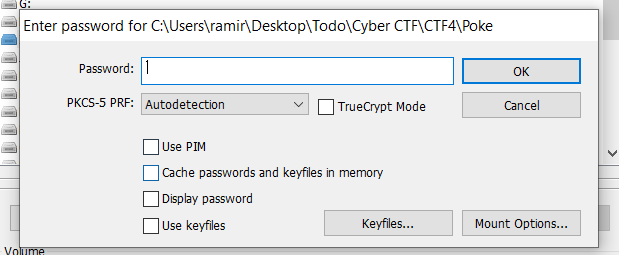
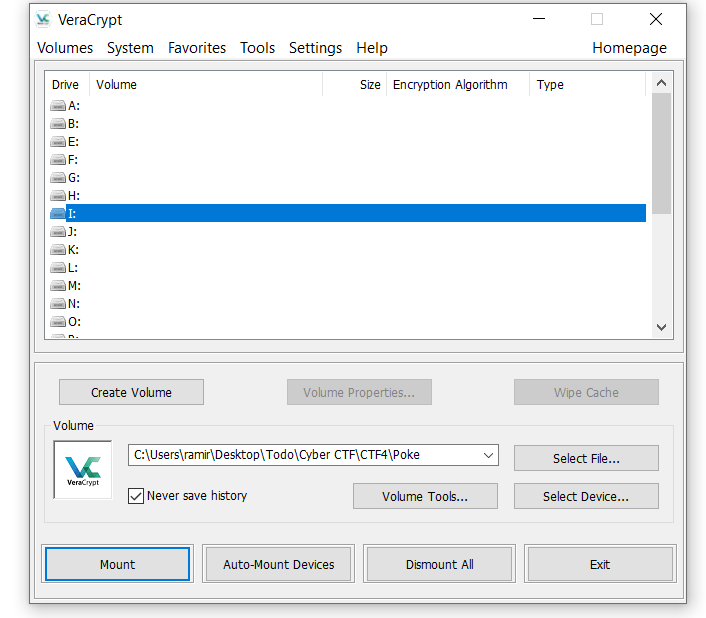
נשים לב כי אנו מדייקים באורך הקטע המודגש (הוא מצוין בHEX). 28 ו 18 בהתאמה שהם שווים בדיוק 40 בתים ו24 בתים בhex בהתאמה!

נייצר קובץ חדש עם הבתים המודגשים ונשמור בשם Poke-unknown.

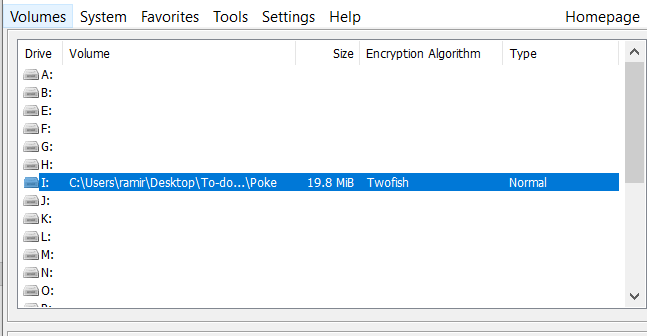
* עד כה נגענו בכל הקבצים חוץ מאחד! הפוכדור!
* נפתח אותו גם כן עם HxD ונגלה בסופו קובץ גדול במיוחד.
* ממש לאחר סימון IEND נראה כי מופיע קטע טקסט decryptfromhere.

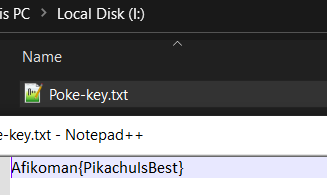


* את כל הקטע שלאחריו נשמור בקובץ חדש ונקרא לו tobedecrypted..
* כעת יש לנו קובץ גדול שאמורים לפענח, רמז לשימוש בהצפנה מסוג two-fish , וקובץ שאיננו יודעים ממש מהו ונסיק כי הוא המפתח שלנו !
* לפענוח הקובץ נשתמש בתוכנה בשם Veracrypt!
* התוכנה משמשת ליצירת קונטיינרים מוצפנים בשלל סוגי הצפנה בינהם גם two-fish.
* נפתח את הקונטיינר שלנו tobedecrypted (קראתי לו poke באתגר עצמו) באמצעות התוכנה ונלחץ mount.



* נכניס את הקובץ שמצאנו מקודם וקראנו לו poke-unknown בתור קובץ מפתח ונקבל לאחר מספר שניות את הכונן החדש שלנו מפוענח.



* ניתן לראות כי התוכנה פענחה את הכונן וזיהתה כי מדובר בהצפנת Twofish.
* לחיצה כפולה על הכונן תפתח אותו ובתוכו נמצא קובץ טקסט עם הפיתרון שלנו.

**Afikoman{PikachuIsBest}**