

תרגיל שחזור קובץ מחוק

קבצי VHD הם קבצי Virtual Hard-Disk שניתנים לטעינה ב-Windows. למעשה, מדובר בקובץ שמעליו בנויה מערכת קבצים, וניתן לעבוד מולם כמו מול דיסק רגיל. על מנת לטעון קובץ VHD יש להשתמש או בממשק ה-Command line של תוכנת DiskPart, או בממשק הגרפי של diskmgmt.msc.

על מנת לטעון את קובץ ה-VHD בעזרת ה-Command Line יש להריץ את הפקודות הבאות מתוך CMD שרץ בהרשאות Administrator (שימו לב, פקודות שלפניהן יש `diskpart` אומרות שמדובר בפקודה לתוכנה `diskpart` ולא בפקודות `cmd` סטנדרטיות)

```
diskpart
```

```
diskpart> select vdisk file="D:\temp\FatFs.vhd"
```

```
diskpart> attach vdisk
```

על מנת לנתק את ה-VHD יש להריץ לאחר מכן את הפקודות

```
diskpart> detach vdisk
```

```
diskpart> exit
```

כעת, ביכולתנו לטעון את הדיסק. בתרגיל זה נעבוד מעל הדיסק שנמצא ב-Rar הנקרא FatFs. שימו לב, הדיסק המדובר מכיל מערכת קבצים מסוג FAT32.

לאחר שנסתכל בתוכן הדיסק, נראה כי קיים בפנים קובץ zip עם שם מעניין (password.zip). אם ננסה לפתוח אותו ולחלץ מתוכו את הקובץ password.txt, נראה כי הzip מוצפן ואנו לא יכולים להוציא מתוכו את המידע.

הרבה פעמים כאשר יוצרים קובץ zip – שמים את כל הקבצים באותה תיקייה, ולאחר יצירת ה zip מוחקים אותם. אולי זה גם המקרה כאן?

עכשיו הכדור עובר אליכם! נסו לראות אם אתם מסוגלים לשחזר את הקובץ המחוק (הכוונה היא לשחזר את הקובץ כך שיהיה ניתן לגשת אליו מתוך Windows)

לצורך התרגיל, נסו להשתמש ב-Hex Editor ובתוכנת DiskEditor (התוכנה יודעת להציג את הקובץ המחוק מראש, המטרה של התרגיל היא לשחזר את הקובץ באמת על ידי שינוי המידע שבדיסק – כך שגם Windows ידע לגשת לקובץ ולא רק התוכנה).