



מעבדה 2



CSRP

DFIR

מבוא ל-DFIR חקירת דליפת נתונים

- עמוד 1 -

כל הזכויות שמורות © סיבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

נושאי המעבדה

שחזרו קבצים מתמונה חשודה של כונן USB והוכח שהם שומשו לגניבת מידע רגיש.

זמן מוערך

20-30 דקות.

סביבת המעבדה

- סביבה וכלים
 - Windows ○
 - PhotoRec ○
 - HashMyFiles ○
 - Exiftool ○
- קבצים
 - Evidence.zip ○
 - testdisk-7.2-WIP.win.zip ○
 - hashmyfiles-x64.zip ○
 - exiftool-11.81.zip ○

משימת מעבדה:

דליפת נתונים קרתה בארגון שלחה. המנכ"ל נותן לך כונן נייד שנמצא בסביבה, והוא חושד שכונן נייד זה שימש להדלפת מסמכים רגישים. המנכ"ל מבקש ממך למצוא את הקבצים המקוריים שהודלפו ואת הבעלים של הכונן.

שחזרו את הנתונים מהכונן הנייד ומצא את בעליו.

תיקיית ה-"Evidence" (ראיות) כוללת את התמונה שהודלפה והעתק גולמי של הכונן הנייד. שחזרו את התמונה שהודלפה, נתחו את ה-metadata של התמונה כדי לראות אם הוא מתאים לקובץ המודלף, והשיגו מידע על הבעלים.

- 1 חלצו את הנתונים מהקובץ הגולמי בכונן – התמונה, בעזרת PhotoRec.
- 2 השוו בין ה-hash של הקובץ המודלף וקבצים חשודים כדי לבדוק אם הם זהים.
- 3 נסו למצוא נתונים כלשהם שיכולים להוביל לבעלים של הכונן.
- 4 מי הוא הבעלים של הכונן?