



# מעבדה 3



CSRP

DFIR

## מבוא ל-DFIR

### התקנת סביבה

- עמוד 1 -

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

## נושאי המעבדה

צורו ערכת וסביבת Forensics לשימוש עתידי בשיעורים.

## זמן מוערך

30-45 דקות.

## סביבת המעבדה

- כלים וסביבה
  - VirtualBox
  - SIFT Environment
    - דיסק און קי
    - CAINE ISO
    - Rufus
- קבצים
  - rufus-3.8.exe

## משימת מעבדה:

במעבדה זו, עלייכם להתקין ולבחון סביבת DFIR באמצעות מכונת SIFT שעוצבה במיוחד לבדיקת קבצים זדוניים.

מעבדה זו גם תסביר כיצד ליצור מכשיר CAINE שניתן לאתחול חוזר ובדוק כלי CAINE, כדי ליצור ערכת שדה (field kit)

- 1 הורידו את הקובץ SIFT OVA מקורס "Resources" ב-LMS שלך.  
שם משתמש: **sansforensics**  
סיסמה: **forensics**
- 2 ייבאו את ה-OVA אל ה-VirtualBox.
- 3 הורידו את הקובץ CAINE.iso מקורס "Resources" ב-LMS שלכם.
- 4 ודאו שהכונן הנייד שאתה רוצה להשתמש בו הוא ריק. אם לא, תמחקו את תוכנו.
- 5 השתמשו בכלי Rufus כדי ליצור מדיה ניתנת לאתחול באמצעות ה-CAINE ISO.
- 6 בדקו עם אילו כלים אתה יכול להשתמש על הכונן.
- 7 אתחלו את תמונת ה-CAINE.
- 8 פתחו את CAINE LIVE ולחצו על התפריט הראשי.
- גשו אל- **Disks <- Accessories**.
- חקורו את התוכן של התכנית Disks, והסבירו מה אתה רואה.
- 9 בתפריט הראשי, בחרו Forensics Tools, ולחצו **XAll**.  
מה זה XAll? הסבירו מה אתה רואה.