



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

צרו 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, עליכם להתקין ולבחון סביבת DFIR באמצעות מכונת SIFT שעוצבה במיוחד לבדיקת קבצים זדוניים.

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

1 הורד את הקובץ SIFT OVA מהמודל.

שם משתמש: **sansforensics**

סיסמה: **forensics**

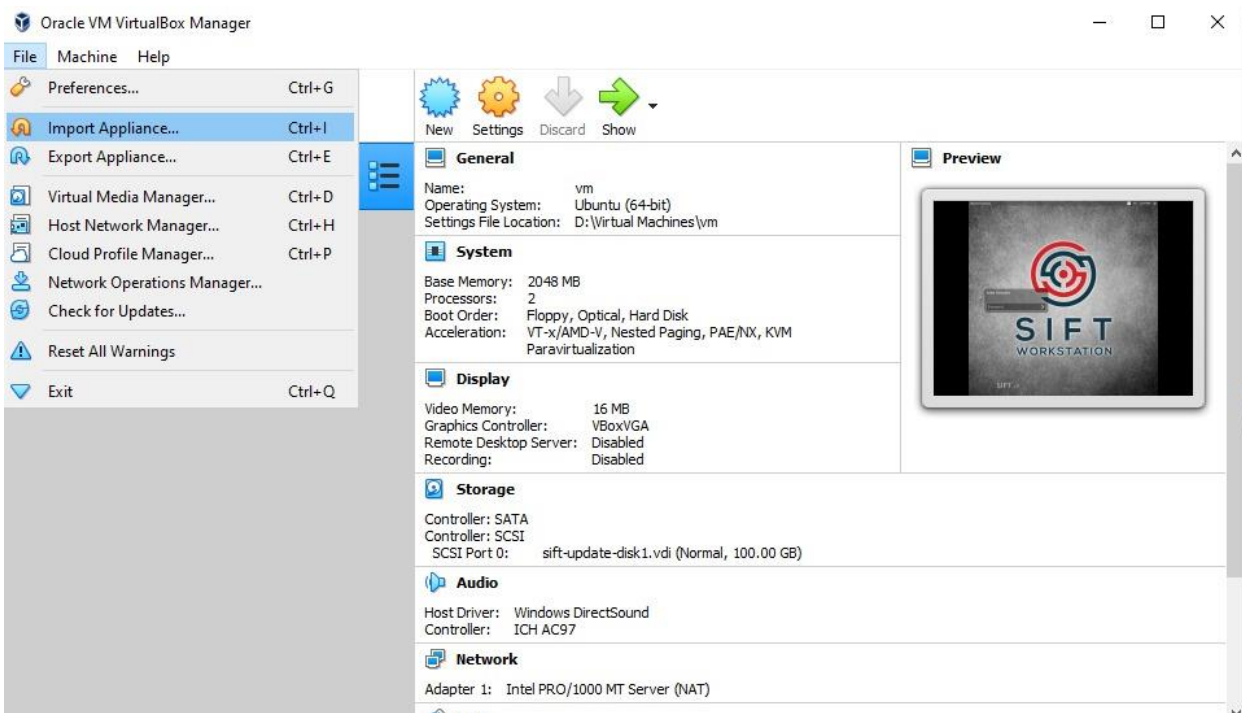
2 ייבאו את ה-OVA אל ה-VirtualBox.

פתרון:

ייבאו את ה-OVA למכונה הוירטואלית Oracle באמצעות

File -> Import Appliance -> File Location -> Location

והתחלו את המכונה.



ברירת המחדל של הסיסמה למשתמש היא: **forensics**

3 הורידו את הקובץ CAINE.iso מהמודל.

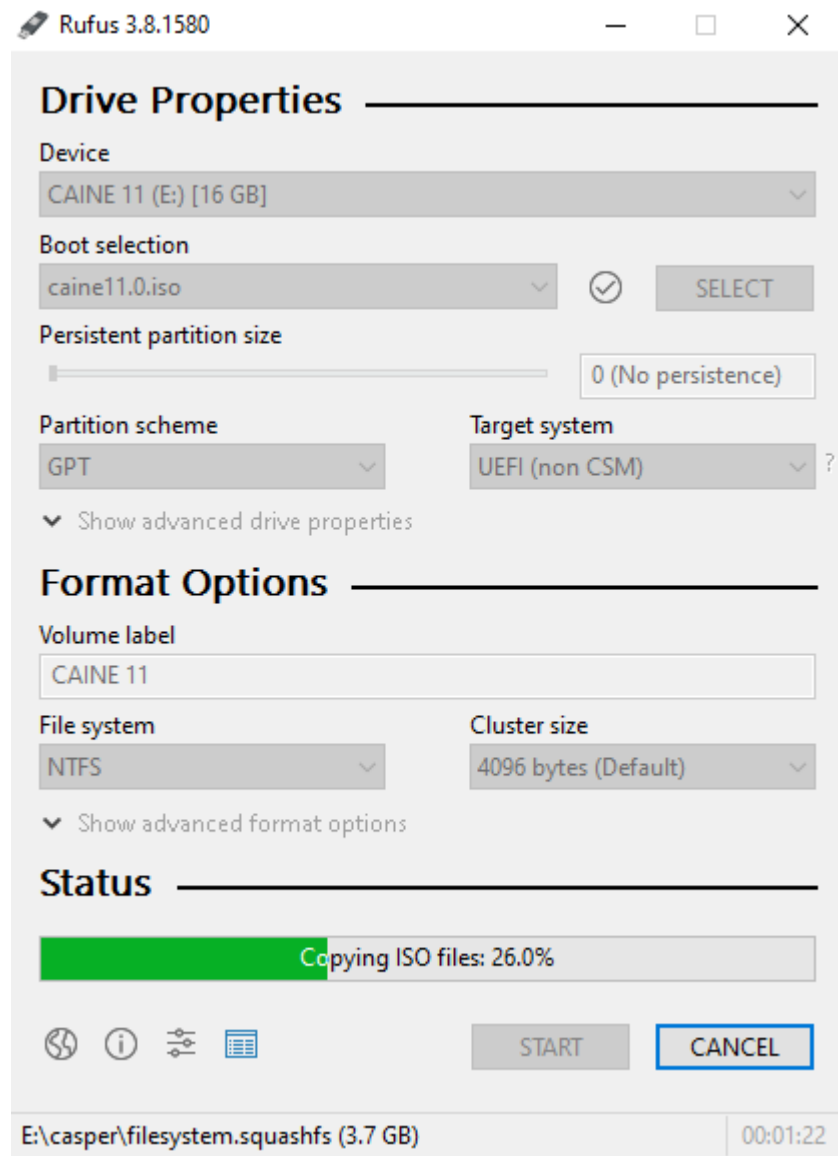
4 ודא שהכונן הנייד שאתם רוצים להשתמש בו הוא ריק. אם לא, תמחקו את תוכנו.

פתרון:

כדי למחוק הכול, לחץ לחיצה ימנית על ה-USB ובחר **Format -> Start**.

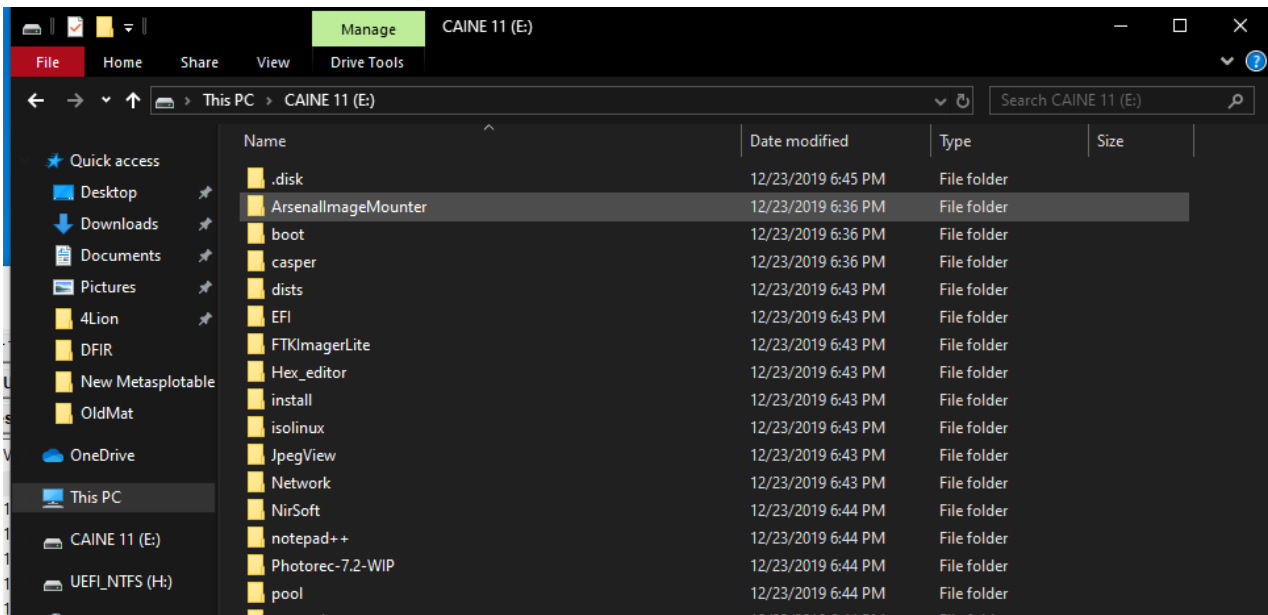
השתמשו בכלי Rufus כדי ליצור מדיה ניתנת לאתחול באמצעות ה-CAINE ISO.
פתרון:

- הריצו את Rufus והגדירו את המידע הבא:
- Device – וודאו שמכשיר ה-USB הוא נכון.
- Boot Selection – וודאו ש-CAINE ISO נבחר.
- Partition scheme – GPT
- Target System – UEFI (non CSM)

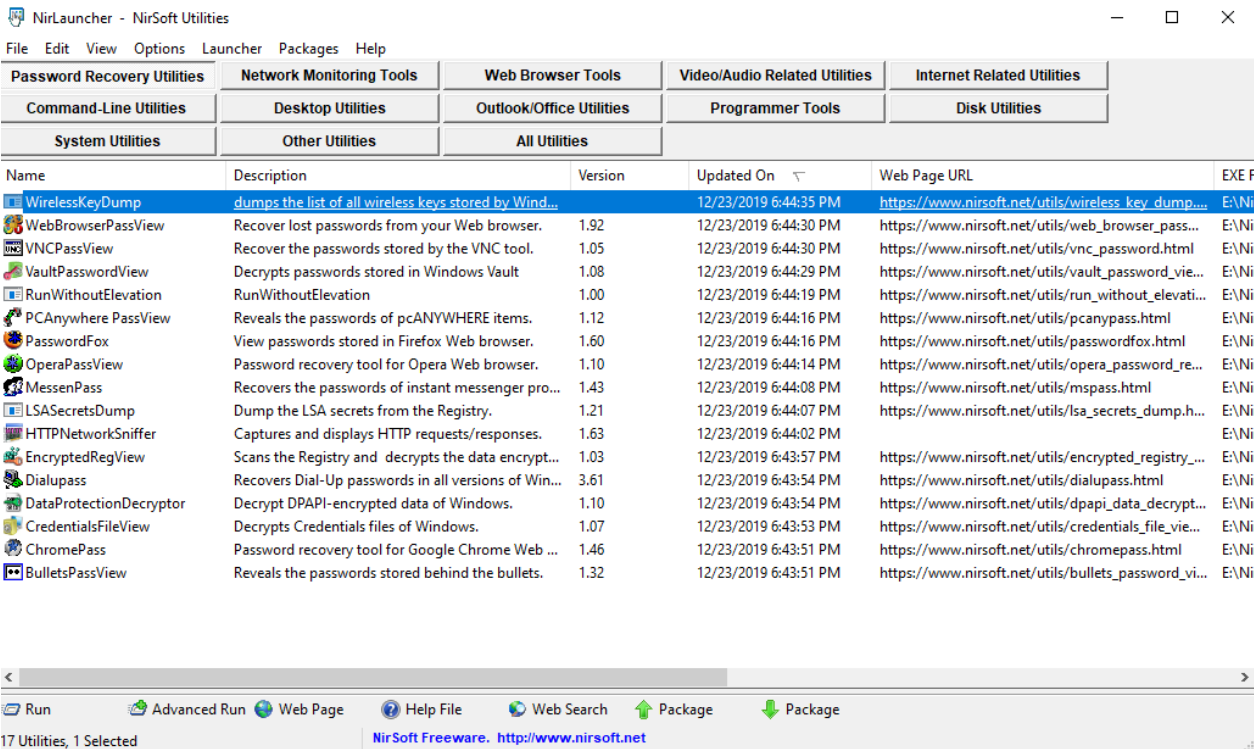


עם ערכי ברירת מחדל בשאר האפשרויות, לחץ Start.
כאשר התהליך מסתיים, ה-USB החדש יהיה Caine USB Live.
בדקו עם אילו כלים אתם יכולים להשתמש על הכונן.

פתרון:
ה-USB שניתן לאתחול החדש אמור להופיע כדיסק חדש במחשב המקומי (local PC).



אתם אמורים לראות כלים רבים, כגון PhotoRec, FTK Imager ואחרים.
הכניסו את הדיסק, והתחלו את NirLauncher כדי לצפות בתוכנות נוספות.



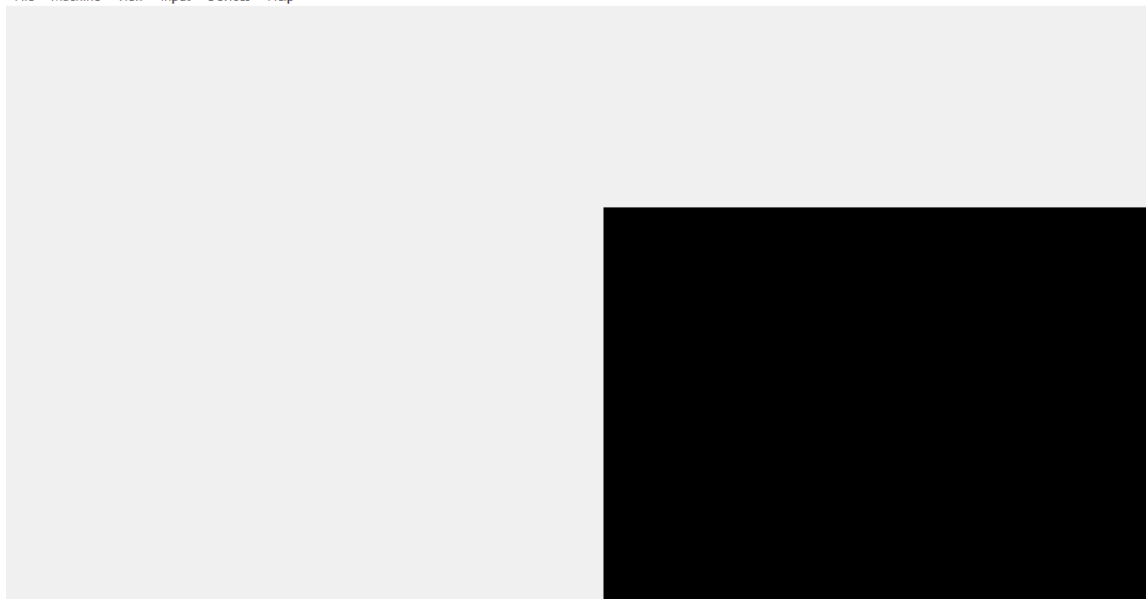
7 אתחלו את תמונת ה-CAINE.

פתרון:

כדי להימנע מאתחול מחדש של כל המחשב, השתמש ב-ISO.
במכונה הוירטואלית, היכנס ל-VirtualBox ולחץ על כרטיסיית Devices.

- עמוד 5 -

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



לחץ Optional Drives, בחר את תמונת דיסק CAINe, ואתחל מחדש את המכונה שלך.

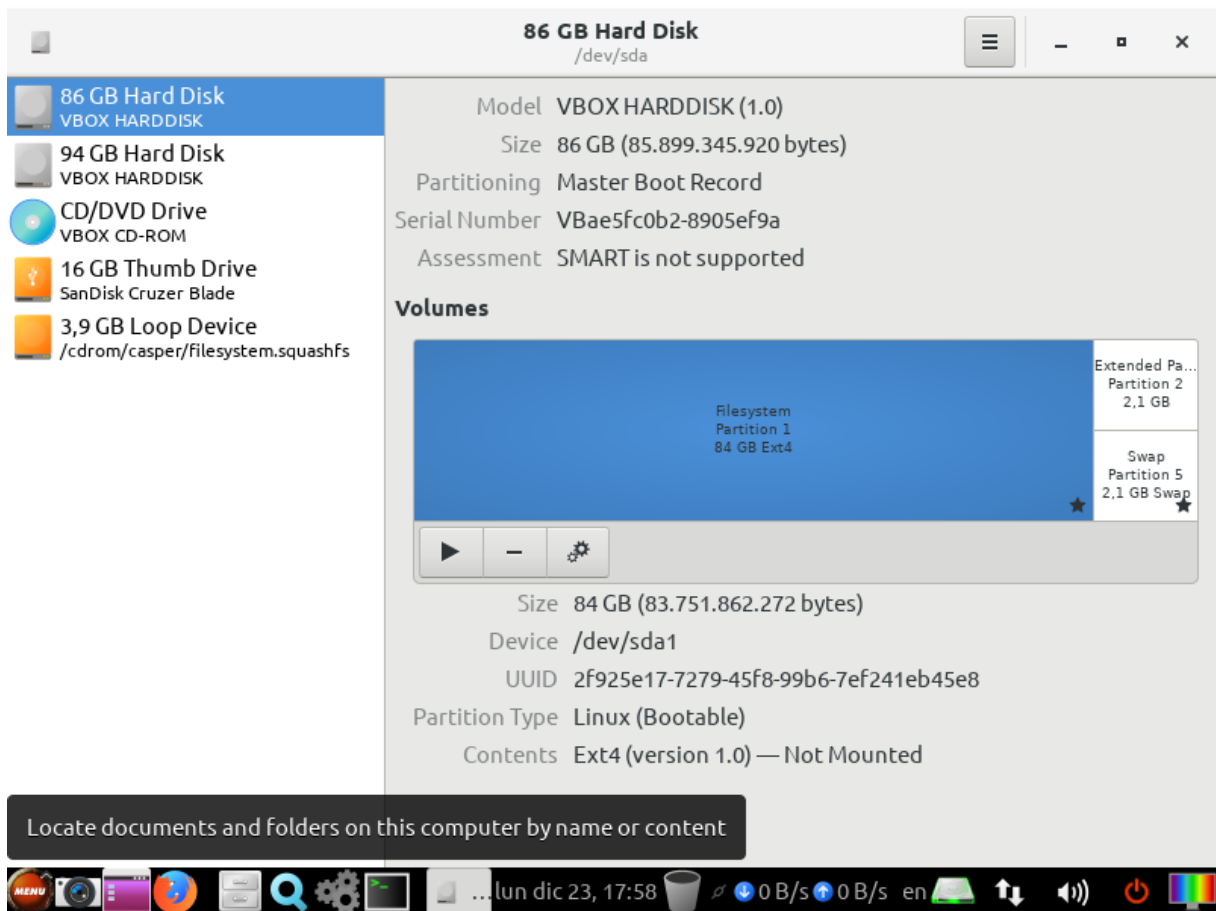


8 פתח את CAINe LIVE ולחץ על התפריט הראשי.

גש אל- **Disks <- Accessories**.

חקור את התוכן של התכנית Disks, והסבר מה אתה רואה.

פתרון:



אתם תראו את כל כונני הזיכרון במחשב שלכם. המידע יכלול את מודל כונן הזיכרון, גודלו, וכמה שטח זיכרון נותר.

בתפריט הראשי, בחרו Forensics Tools, ולחצו XAII. 9
מה זה XAII? הסבירו מה אתם רואים.

תפריט:

XAII הוא כלי שיכול לחלץ את כל הקבצים ממכשירים, כולל קבצי תמונות. אתם תראו עץ מערכת הקבצים, ותצטרפו לבחור תיקייה או קובץ תמונה כדי לחלץ את התוכן שלו.