מעבדה 2

CSRP

DFIR

מבוא ל-DFIR

חקירת דליפת נתונים

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

נושאי המעבדה

שחזר 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

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

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.

שחזר את הנתונים מהכונן הנייד ומצא את בעליו.

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

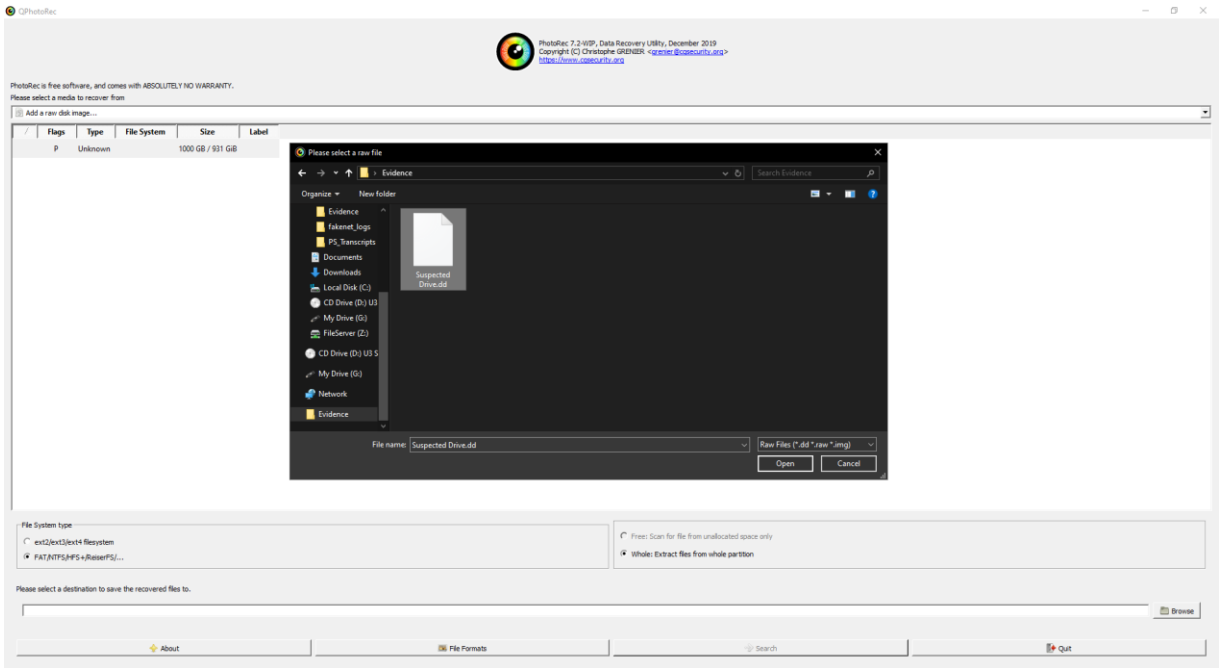
שים לב: צילומי המסך בפתרונות מציגות תמונה שונה. זה בסדר.

1. חלץ את הנתונים מהקובץ הגולמי בכונן – התמונה, בעזרת PhotoRec.

פתרון:

פתח את גרסת ה-GUI של PhotoRec. אתה יכול גם להשתמש בגרסת ה-CLI, אבל עדיף להשתמש ב-GUI.

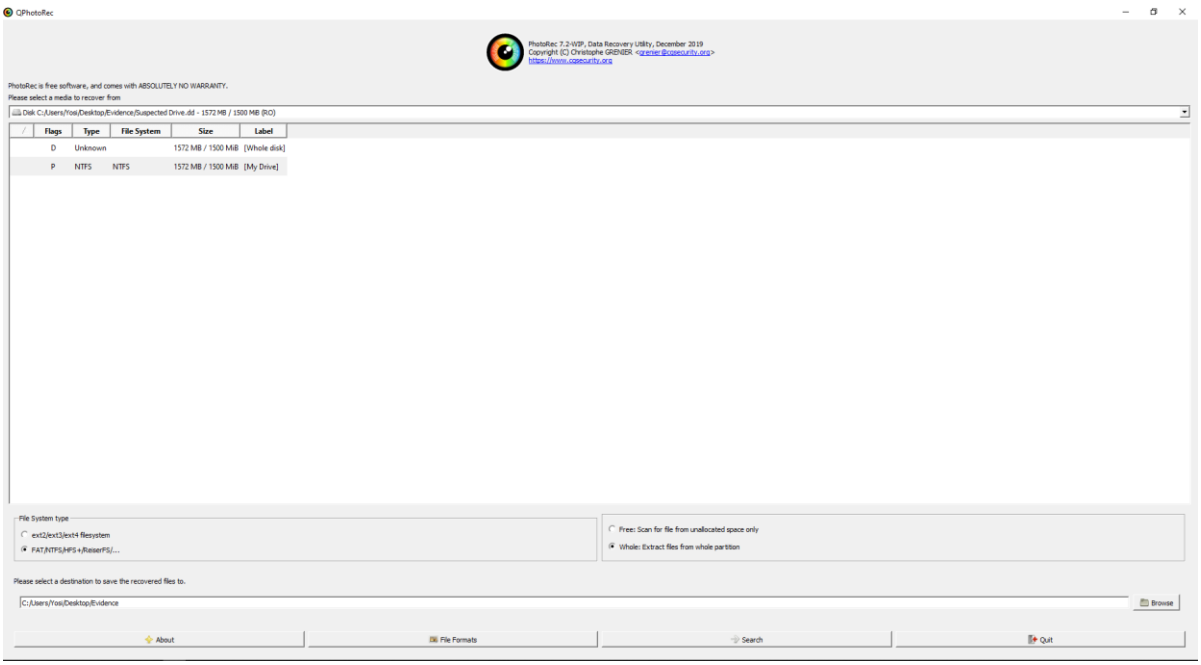
עבור Select a media to recover, בחר Add a raw disk image. לאחר מכן בחר את התמונה הגולמית הממוקמת בתיקיית Evidence.



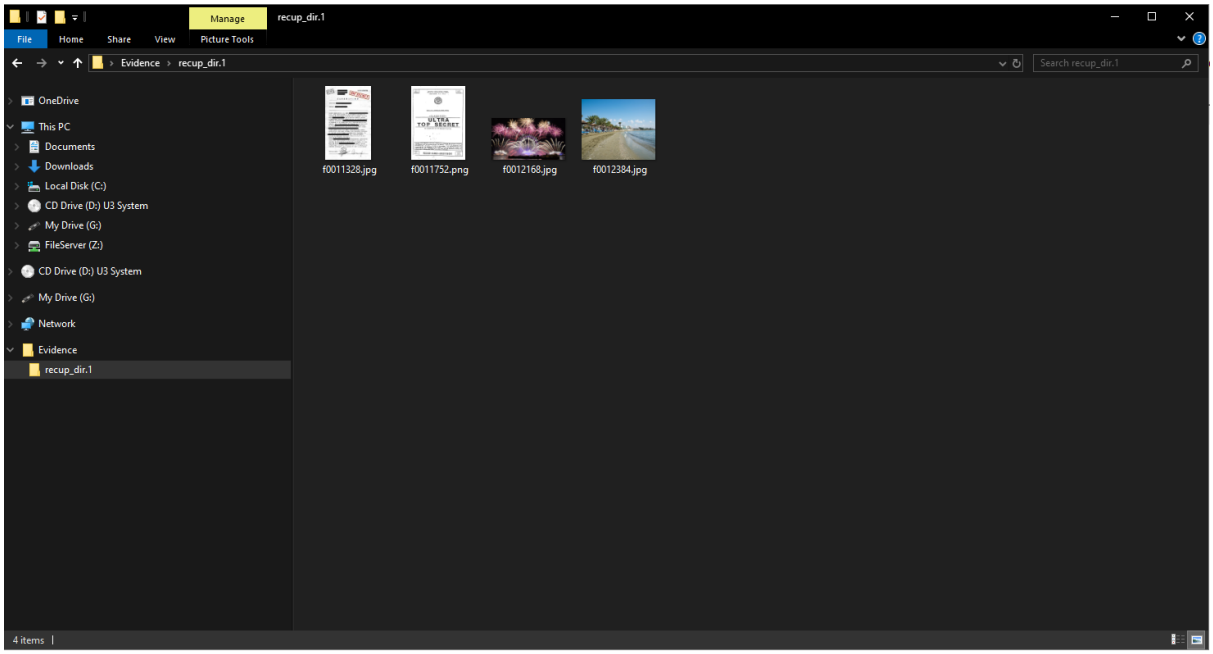
חלץ את כל התמונה ע"י בחירה ב-Whole: Extract files from whole partition.

בחר יעד לחילוץ הקבצים, ולחץ Search.

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



חכה עד שההליך יסתיים, ואז פתח את תיקיית היעד כדי לראות את התמונה המשוחזרת.
בתיקיית היעד נוצרה תיקייה חדשה בשם "recup_dir.1".

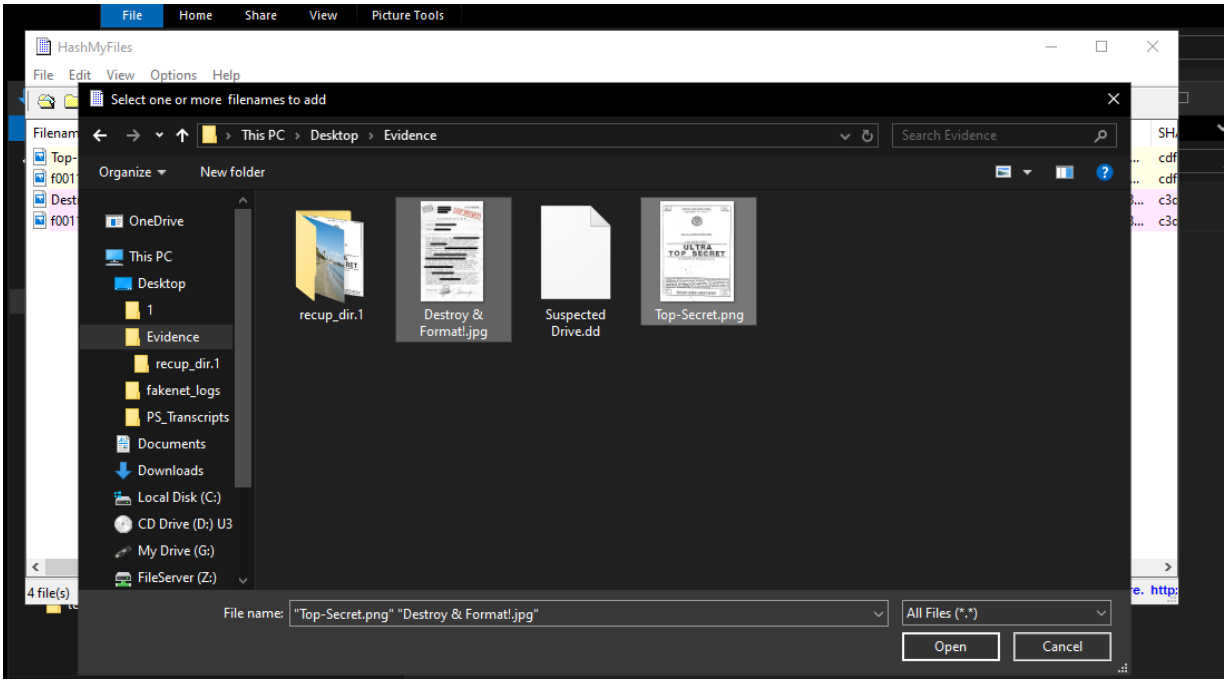


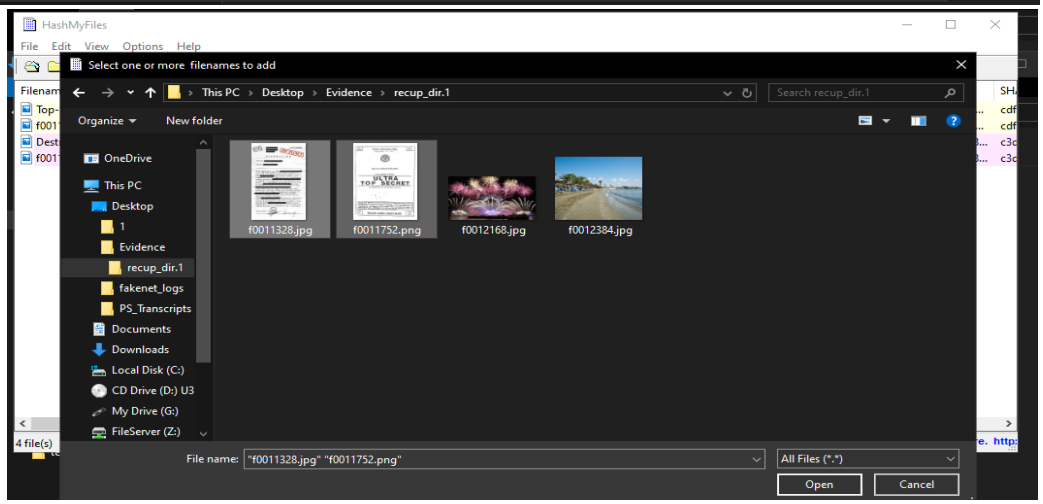
2 השווה בין ה-hash של הקובץ המודלף וקבצים חשודים כדי לבדוק אם הם זהים.

פתרון:

הרץ HashMyFiles.exe, פתח את הקובץ המודלף בתיקיית Evidence, ופתח את הקבצים המודלפים החשודים מהתמונה המשוחזרת.

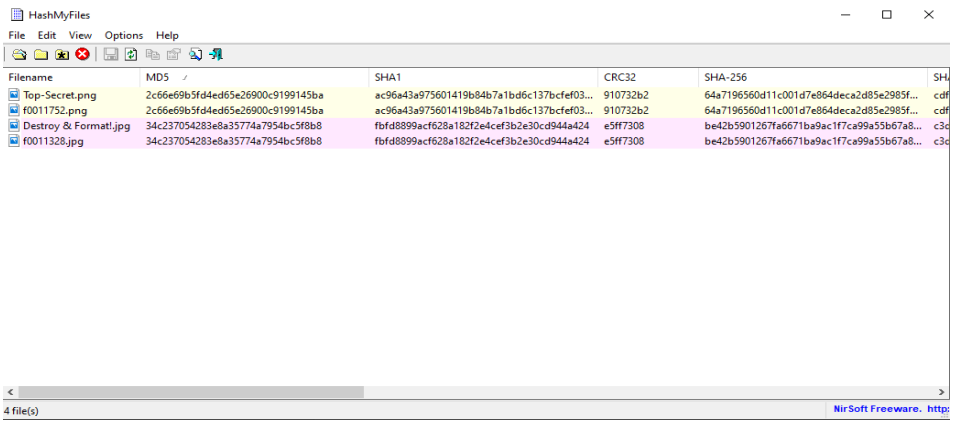
כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383





השווה את ה-hashes של הקבצים.

אם ה-hashes זהים, הקבצים גם הם זהים, וההדלפה אומתה.



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

CYBER SCHOOL

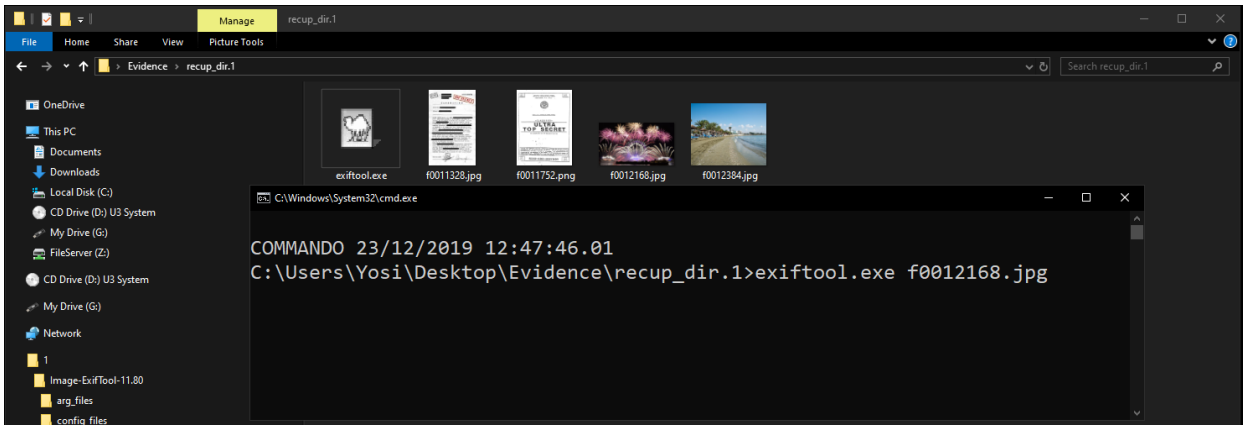
3 נסה למצוא נתונים כלשהם שיכולים להוביל לבעלים של הבונן.

פתרון:

שים לב שתמונות אישיות בבונן המשוחזר כוללת metadata על הבעלים. מציאת הנתונים תחשוף את זהות בעלי הבונן.

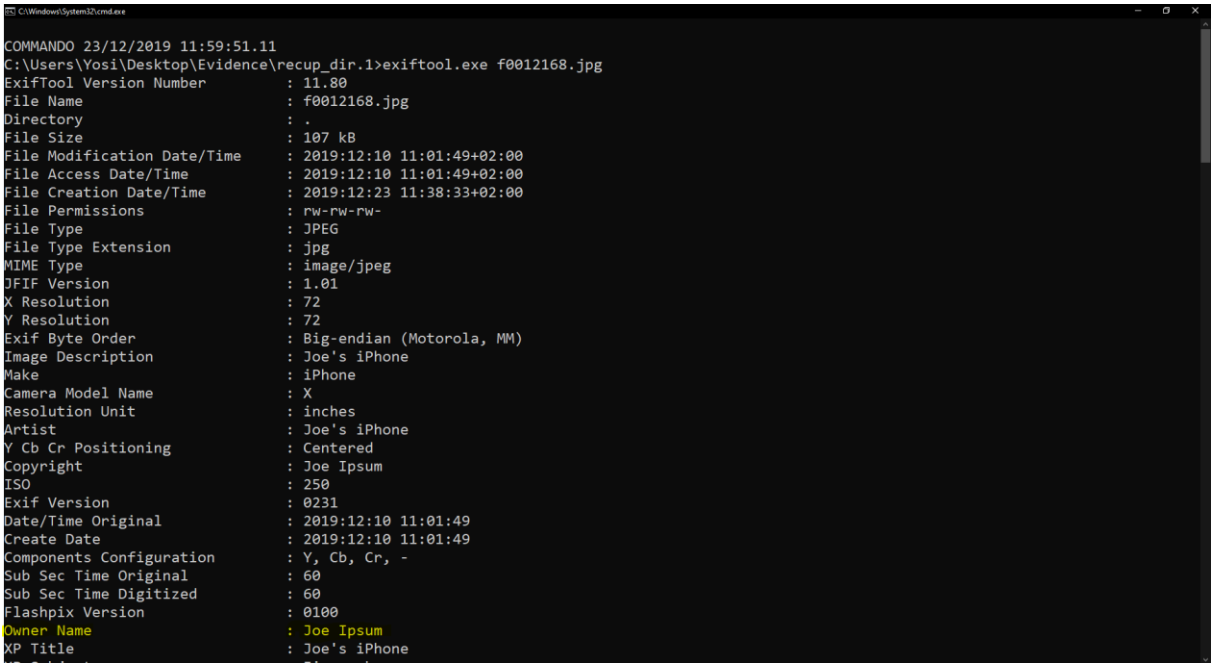
הזז את exiftool.exe אל התיקייה שכוללת את הקבצים המשוחזרים, פתח את שורת הפקודה בתיקייה, והרץ את הפקודה הבאה (השלם את שם הקובץ בסוגריים המרובעים):

exiftool.exe [name of file to test]



אחרי ביצוע הפקודה, מידע meta יוצג.

חפש את החלק עם שם הבעלים כדי לחשוף את השם.



4 מי הוא הבעלים של הבונן?

פתרון:

הבעלים הוא ג'ו איפסום – Joe Ipsum.

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