

CSRP **DFIR**

DFIR-מבוא ל חקירת דליפת נתונים



- עמוד 1 -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.



20-30 דקות.



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



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.

CPHOLONEC			
	PhotoRe: 7.3-949P, Da Copyright (C) Christoph https://www.caecurit	ta Recovery Utility, December 2019 te GRHIBER < desenutiv.arg > 1.00	
PhotoRec is free software, and comes with ABSOLUTELY NO WARRANTY.			
Please select a media to recover from			
Add a raw disk image			
/ Flags Type File System Size Label			
P Unknown 1000 GB / 931 GiB	Please select a raw file	×	
+	→ 👻 🕇 🔜 > Evidence	v ð Search Evidence Ø	
0	rganize 🖛 New folder	🖬 - 🔳 🚷	
	E rodence A E rodence A P 75,5mcrepts B Counted C CDDwr (b) C P MDwr(c) B Felderec C C CDDwr (b) US 5 P MDwr(c) B Felderec C C Solution C C Colone (b) US 5 P MDwr(c) B Felderec C		
	File name: Supersted Drive dd	Paur Eller (* dd * rau * ima)	
		Open Cancel	
		<i>_</i>	
File System type			
C ext2/ext3/ext4 filesystem		rree: scan for the from unanocated space only	
FAT_NTFS_MFS+/ReiserFS/		(Whole: Extract files from whole partition	
Please select a destination to save the recovered files to.			
			Erowse
🔶 About	🐹 File Formats		🚺 Quit

חלץ את כל התמונה ע"י בחירה ב-Whole: Extract files from whole partition. בחר יעד לחילוץ הקבצים, ולחץ Search.



QPhotoRec	Ghiotelic – O X						
					PhotoRec: 7.3-VVP, Do Coovright (C) Orivitos https://ivon.coecurit	ta Recovery Utility, December 2019 he GROER < <u>commer Biosecurity.cc</u> > LOIS	
PhotoRec is free sof Please select a medi	tware, and co a to recover fi	mes with ABSOLUTE	ELY NO WARRANTY.				
Disk C:/Users/Y	186 246C2 97020 1980 19820 19820 19820 1982 1982 1982 1982 1982 1982 1982 1982						
/ Flags	Type	File System	Size	Label			
D	Unknown		1572 MB / 1500 MiB	[Whole disk]			
P	NTFS	NTES	1572 MB / 1500 MiB	8 [My Drive]			
File System type	File System type						
C ext2/ext3/e	kt4 filesystem					Whole: Extract files from whole partition	
Please select a des	Pass select a distribution to save the recovered first to.						
[c./Jaen/vos/bestup[b/dance							
							-
		🔶 Aboi	ut		Di File Formats	> Search	Duit Quit

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.





File name: "f0011328.jpg" "f0011752.png"

4 file(s)

Open השווה את ה-hashes של הקבצים.

e. http

٦

Cancel

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

HashMyFiles				- U	×
File Edit View Option:	s Help				
🛳 🗀 鮱 🔕 🔜 😰	Pa 🗊 🔕 📲				
Filename	MD5 2	SHA1	CRC32	SHA-256	SH
Top-Secret.png f0011752.png Destroy & Formatl.jpg f0011328.jpg	2c66e69b5fd4ed65e26900c9199145ba 2c66e69b5fd4ed65e26900c9199145ba 34c237054283e8a35774a7954bc5f8b8 34c237054283e8a35774a7954bc5f8b8	ac96a43a975601419b84b7a1bd6c137bcfef03 ac96a43a975601419b84b7a1bd6c137bcfef03 fbfd8899acf628a182f2e4cef3b2e30cd944a424 fbfd8899acf628a182f2e4cef3b2e30cd944a424	910732b2 910732b2 e5ff7308 e5ff7308	64a7196560d11c001d7e864deca2d85e2985f 64a7196560d11c001d7e864deca2d85e2985f be42b5901267fa6671ba9ac1f7ca99a55b67a8 be42b5901267fa6671ba9ac1f7ca99a55b67a8	cdf cdf c3c c3c
<					>
A file(c)				NirSoft Freeware.	http:



נסה למצוא נתונים כלשהם שיכולים להוביל לבעלים של הכונן. **3**

פתרון:

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

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.

E: C:\Windows\System32\cmd.exe	
COMMANDO 23/12/2019 11:59:51	11
C:\Users\Yosi\Deskton\Evidenc	alrecun dir 12exiftool exe f0012168 ing
ExifTool Version Number	
File Name	: f0012168, ing
Directory	
File Size	- 107 kB
File Modification Date/Time	· 2010-12-10 11-01-49+02-00
File Access Date/Time	: 2019:12:10 11:49:49:20
File Creation Date/Time	: 2019:12:23 11:38:33-02:00
File Permissions	
File Type	: JPEG
File Type Extension	; jpg
MIME Type	: image/ipeg
JFIF Version	: 1.01
X Resolution	: 72
Y Resolution	: 72
Exif Byte Order	: Big-endian (Motorola, MM)
Image Description	: Joe's iPhone
Make	: iPhone
Camera Model Name	: X
Resolution Unit	: inches
Artist	: Joe's iPhone
Y Cb Cr Positioning	: Centered
Copyright	: Joe Ipsum
ISO	: 250
Exif Version	: 0231
Date/Time Original	: 2019:12:10 11:01:49
Create Date	: 2019:12:10 11:01:49
Components Configuration	: Y, Cb, Cr, -
Sub Sec Time Original	: 60
Sub Sec Time Digitized	: 60
Flashpix Version	: 0100
Owner Name	: Joe Ipsum
XP Title	: Joe's iPhone

4 מי הוא הבעלים של הכונן? פתרון: הבעלים הוא ג'ו איפסום – Joe Ipsum.

