Machine Translated by Google

תיעוד TestDisk

מהדורה 7.2

כריסטוף גרנייר

9במאי 2024

Machine Translated by Google

Machine Translated by Google

תוֹכֶן

1 מצגת . . . 3
1.1 TestDisk - שחזור מחיצות . . . 4
1.2 TestDisk - תיקון מערכת קבצים . . . 5
1.3 TestDisk - שחזור קבצים . . . 5
1.4 PhotoRec - שחזור קבצים . . . 6
1.5 QPhotoRec - שחזור קבצים . . . 6

2 התקנה . . . 7
2.1 לינוקס: התקנה של חבילת הפצה . . . 7
2.2 macOS: התקנה באמצעות Homebrew . . . 8
2.3 קבצים בינאריים רשמיים . . . 9

3 בנייה ממקור . . . 11
3.1 סביבת קומפילציה . . . 11
3.2 סביבת קומפילציה צולבת . . . 13
3.3 קומפילציה . . . 13

4 יצירת USB חי . . . 15
4.1 Windows . . . 15
4.2 לינוקס (שורת פקודה) . . . 15
4.3 לינוקס (GNOME) . . . 16
4.4 OS X . . . 16
4.5 החל ממקל ה-USB . . . 16

5 אחסון: האם אני יכול לתקן אותו או לשחזר ממנו נתונים? . . . 17

6 הפעלת הכלים . . . 19
6.1 תמונת דיסק . . . 19
6.2 הפעלת TestDisk, PhotoRec או QPhotoRec תחת Windows . . . 19
6.3 הפעלת TestDisk, PhotoRec תחת Linux . . . 20
6.4 הפעלת QPhotoRec תחת Linux X.org X11 . . . 20
6.5 הפעלת QPhotoRec תחת Linux Wayland . . . 20
6.6 הפעלת TestDisk, PhotoRec תחת macOS . . . 20
6.7 הפעלת Fidentify תחת Windows . . . 21
6.8 הפעלת Fidentify תחת לינוקס או macOS . . . 21

7 תיקון מערכת קבצים . . . 23
7.1 תיקון מערכות קבצים מ-Windows . . . 23
7.2 תיקון מערכות קבצים מ-Linux . . . 23
7.3 תיקון מערכות קבצים מ-macOS . . . 23
7.4 תיקון מגזר האתחול של FAT32, exFAT ו-NTFS באמצעות TestDisk . . . 24

Machine Translated by Google

תיקון מגזר האתחול של FAT 7.6 TestDisk: תיקון מגזר האתחול 7.5 TestDisk: . . . 24
. מערכת הקבצים של ext2/3/4 superblock תיקון NTFS 7.7 TestDisk: . . . 25
. . . 25
BitLocker . תיקון נפח TestDisk 7.9 באמצעות HFS/HFS+ תיקון כותרת נפח 7.8 . . . 26
. . . 27

8 שחזור קבצים שנמחקו באמצעות TestDisk 29
exFAT, ext2 8.2 TestDisk: ביטול מחיקת קובץ עבור 8.1 TestDisk: . . . 29
NTFS . ביטול מחיקת קובץ עבור FAT, . . . 31

9 שחזור מחיצה שנמחקה באמצעות testdisk 9.2 התחל TestDisk 9.1 33
ניתוח 9.5 מחיצות עבור רוט 9.4 בחירת סוג מחיצה 9.3 בחירת דיסק 9.6 . . . 33
. . . 33
. . . 33
. . . 34
. . . 34
. . . 34
בחירת מחיצות 9.8 . חפש מחיצות נוספות 9.7 . . . 35
. . . 35

10 כיצד להפוך את המערכת לניתנת לאתחול מחדש - 95/98 . חלון 10.1 DOS 37
. . . 37
10.2 Windows 2000/XP/2003 . . . 37
10.3 Windows Vista/Windows 7/. . . , Windows Server 2008/. 37
לינוקס/ FreeBSD. . 10.4 . . . 38

11 שחזור קבצים שנמחקו באמצעות PhotoRec 39
בחירת מחיצת מקור 11.3 בחירת דיסק PhotoRec 11.2 התחל את 11.1 . . . 39
PhotoRec . אפשרויות 11.4 . . . 39
. . . 39
. . . 40
בחירת קבצים לשחזור 11.5 . . . 40
סוג מערכת הקבצים 11.6 . . . 40
. לחצוב את המחיצה או את החלל הלא מוקצה בלבד 11.7 . . . 41
. בחר היכן יש לכתוב קבצים משוחזרים 11.8 . . . 41
שחזור מתבצע 11.9 . . . 41
השחזור הושלם 11.10 . . . 42
תואם שם הקובץ 11.12 PhotoRec: שם קובץ ותאריך 11.11 PhotoRec: . . . 42
ומיקום הנתונים . . . 43

12 יצירת חתימה מותאמת אישית עבור PhotoRec 12.1 Signature Syntax . 45
. . . 45
בדוק את החתימה המותאמת אישית שלך עם 12.3 מיקום הקובץ 12.2 . . . 46
fidentify 46
. קבצים משופר שחזור PhotoRec 12.5 . הפעל את 12.4 . . . 47
. . . 47

13 שחזור סרטונים שאבדו מכרטיס זיכרון באמצעות PhotoRec 49

14 לאחר שימוש במיון הקבצים לפי-PhotoRec 14.1 51
14.3 שינוי שמות של קבצים באמצעות 14.2 סיומת . . . 51
הסרת קבצים משוכפלים exiftool . . . 51
. . . 52

15 מצב - ניטור בריאות הדיסק SMART 53

Machine Translated by Google

16שחזור נתונים מדיסק פגום DDRescue: 55
.16.2 ddrescue ב-macOS . xuniL.ב16.1 ddrescue 55
. . . . 55
. תמונת דיסק לקובץ16.3 DDRescue: 56
לבלוק נתוניםddrescue הגבלת16.5 ddrutility: . העתקת דיסק לדיסק16.4 DDRescue: 56
SFTN-שהוקצה ל 56

אוטומציה של שחזורTestDisk 17.2 אוטומציה של שחזור באמצעותScripted 17.1 ריצה17 59
PhotoRec 17.3 Windows UAC . באמצעות 59
. . . . 63
. . . . 66

ביטול מחיקת18.1 DFTT: במקרים שונים של בדיקות פורנזיות דיגיטליות18 TestDisk ו-PhotoRec 67
FAT16 . קבצים ממערכת קבצים 67
NTFS . בטל מחיקת קבצים ממערכת קבצים18.2 DFTT: 68
. . . . לזיהוי פלילי DFRWS 2006 אתגר18.3 69
. . . . . זיהוי פלילי: כתיבת חותמים18.4 71

. . . משתמשים19.2 הפעלת מסוףmacos / BSD 19.1 / שורת הפקודה לינוקס19 73
. . . . 73
. . . . 73
. . . . מערכת קבצים19.3 74
. . . . פקודות19.4 74

Machine Translated by Google

Machine Translated by Google

TestDisk & PhotoRec

https://www. cgsecurity.org/. -הם כלי עזר חינמיים לשחזור נתונים בקוד פתוח. ניתן להוריד אותם מTestDisk ו-PhotoRec

ניתן להשתמש TestDisk-בכדי לשחזר מחיצות שאבדו, לתקן סקטורי אתחול ולשחזר קבצים ממערכות קבצים פגומות או שנמחקו. הוא משמש בעיקר לשחזור נתונים מכוננים קשיחים, אך הוא יכול לעבוד גם עם התקני אחסון אחרים כגון כונני USBוכרטיסי זיכרון. הוא תומך במגוון רחב של מערכות קבצים, כולל .NTFS, exFAT, FAT, ext2, ext3 ו-ext4

PhotoRecנועד לשחזר קבצים שאבדו, כולל תמונות, סרטונים וקובצי מוזיקה, מסוגים שונים של התקני אחסון. זה יכול לשחזר קבצים מכוננים קשיחים, כרטיסי זיכרון וכונני ,USBוהוא יכול גם לשחזר קבצים ממצלמות דיגיטליות והתקנים ניידים אחרים.

Machine Translated by Google

Machine Translated by Google

פֶּרֶק

אֶחָד

הַצָגָה

TestDisk ו-PhotoRecהם כלי עזר חינמיים לשחזור נתונים בקוד פתוח. TestDiskנוצר בשנת 1998 ו-PhotoRec באפריל 2002 על ידי Christophe GRENIER, ניתן להוריד אותם מ- https://www.cgsecurity.org/. הם מופצים תחת GNU General Public License v2 ואילך, אתה יכול

- להפעיל את התוכנית כרצונך, לכל מטרה,
- למד כיצד התוכנית פועלת, ושנה אותה כך שהיא תעשה את המחשוב שלך כרצונך (יש לך גישה למקור קוד.),
- להפיץ מחדש עותקים כדי שתוכל לעזור לשכן שלך,
- להפיץ עותקים של הגרסאות ששוננו לאחרים תחת אותו רישיון. על ידי כך אתה יכול לתת את כל הקהילה הזדמנות ליהנות מהשינויים שלך.

ניתן למצוא תיעוד זה באינטרנט בכתובת https://github.com/cgsecurity/testdisk_documentation. כל אחד יכול לתרום לתיעוד TestDisk ו-PhotoRec. אנו מברכים במיוחד על תרומותיהם של מתחילים. למעשה, למתחילים יש יתרון מובהק על פני המומחים, מכיוון שהם יכולים לזהות ביתר קלות את המקומות שבהם חסר תיעוד. אם זה רק כדי לתקן שגיאת כתיב או דקדוק, גם תרומתך תתקבל בברכה!

ארכיונים עם קבצים בינאריים מוכנים לשימוש זמינים עבור

- DOS (32 סיביות x86)
- Microsoft Windows (32 סיביות x86 או 64 סיביות x64)
- לינוקס (32 סיביות x86 או 64 סיביות x64)
- macOS / Mac OS X (PowerPC או Intel) / OS X
- Marvell 88F628x Linux

ניתן להרכיב TestDisk ו-PhotoRec גם עבור פלטפורמות אחרות, במיוחד

- FreeBSD/OpenBSD/NetBSD, מערכת הפעלה מחשב דמוית Unix שמקורה ב-Berkeley Software Distribution (BSD), נגזרת Research Unix שפותחה באוניברסיטת קליפורניה, ברקלי.
- Haiku, מערכת הפעלה חינמית וקוד פתוח התואמת BeOS-לשהופסק כעת.
- SunOS/Solaris, מערכת הפעלה ממותגת Unix שפותחה על ידי Sun Microsystems עבור מערכות המחשב של תחנות העבודה והשרתים שלה,

1.1 TestDisk - שחזור מחיצות

TestDiskמזהה את חלוקת הדיסק הבאה:

- מפת מחיצות אפל
- טבלת מחיצות GUID
- Humax
- טבלת מחיצות PC/Intel (רשומת אתחול ראשי)
- פרוסת Sun Solaris
- ערכת חלוקה קבועה של Xbox

זה גם מטפל במדיה לא מחולקת.

TestDiskיכול

- לשחזר מחיצה שנמחקה
- לבנות מחדש את טבלת המחיצות
- לכתוב מחדש את רשומת האתחול הראשית (MBR)

TestDiskמבצע בדיקה מהירה של מבנה הדיסק ומשווה אותו לטבלת המחיצות עבור שגיאות כניסה. לאחר מכן, הוא מחפש מחיצות אבודות של מערכות קבצים אלה:

- מערכת קבצים (BeOS)
- תווית דיסק BSD (FreeBSD/OpenBSD/NetBSD)
- Cramfs, מערכת קבצים דחוסה
- DOS/Windows FAT12, FAT16 ו-FAT32
- Windows exFAT
- HFS, HFS+ ו-HFSX, מערכת קבצים היררכית
- IBM Journaled File System 2 (JFS2)
- Linux ext2, ext3 ו-ext4
- Linux RAID
  - RAID 1: שיקוף
  - RAID 4: מערך פסים עם התקן זוגיות
  - RAID 5: מערך פסים עם מידע זוגיות מבוזר
  - RAID 6: מערך פסים עם מידע יתירות כפולה מבוזרת
- Linux Swap (גירסאות 1 ו-2)
- LVM ו-LVM2, Linux Logical Volume Manager
- Novell Storage Services (NSS)
- מערכת קבצים טכנולוגית חדשה של Windows (NTFS)
- ReiserFS 3.5, 3.6 ו-4
- תווית דיסק של Sun Solaris i386
- Unix File System UFS ו-UFS2 (Sun/BSD/. . .)
- XFS, מערכת הקבצים העיתונאית של SGI

Machine Translated by Google

תיקון מערכת קבצים1.2 TestDisk -

יכול להתמודד עם פגיעה מסוימת במערכת הקבצים הלוגית:TestDisk

• טבלת הקצאת קבצים, FAT12 ו-FAT16

- מצא פרמטרים של מערכת הקבצים כדי לשכתב סקטור אתחול חוקי
- השתמש בשני העותקים של FAT-הכדי לשכתב גרסה קוהרנטית

• טבלת הקצאת קבצים, FAT32

- מצא פרמטרים של מערכת הקבצים כדי לשכתב סקטור אתחול חוקי
- שחזר את סקטור האתחול באמצעות הגיבוי שלו
- השתמש בשני העותקים של FAT-הכדי לשכתב גרסה קוהרנטית

• exFAT

- שחזר את סקטור האתחול באמצעות הגיבוי שלו

• NTFS (New Technology File System) סקטור האתחול ותיקון MFT

- מצא פרמטרים של מערכת הקבצים כדי לשכתב סקטור אתחול חוקי
- שחזר את סקטור האתחול באמצעות הגיבוי שלו
- שחזר את טבלת הקבצים הראשית (MFT)מהגיבוי שלה

• מערכות קבצים מורחבות, ext2, ext3 ו-ext4

- מצא מיקום סופרבלוק לגיבוי כדי לסייע ל-fsck

• HFS+

- שחזר את סקטור האתחול באמצעות הגיבוי שלו

שחזור קבצים1.3 TestDisk -

כאשר קובץ נמחק, רשימת אשכולות הדיסקים התפוסים על ידי הקובץ נמחקת, ומסמנת את אותם סקטורים הזמינים לשימוש על ידי קבצים אחרים שנוצרו או שונו לאחר מכן. אם הקובץ לא היה מקוטע ולא נעשה שימוש חוזר באשכולות, TestDiskיכול לשחזר את הקובץ שנמחק עבור מערכות קבצים שונות:

• FAT
• NTFS
• exFAT
• ext2

Machine Translated by Google

1.4 PhotoRec - שחזור קבצים

PhotoRecהוא כלי תוכנה לשחזור נתונים לחוצץ קבצים. זה לא משחזר את שמות הקבצים המקוריים, אבל זה יכול לשחזר קבצים למחוק אפילו ממערכת קבצים פגומה. PhotoRecמזהה ומשחזר פורמטים רבים של קבצים כולל ZIP, Office, PDF, HTML, JPEGופורמטים שונים של קבצים גרפיים. כל הרשימה של פורמטי הקבצים ששוחזרו על ידי PhotoRecמכילה יותר מ-084 סיומות קבצים (כ-003 משפחות קבצים). אפשר ליצור חתימה מותאמת אישית כדי לשחזר פורמט קובץ שאינו ידוע ל-PhotoRec.

1.5 QPhotoRec - שחזור קבצים

QPhotoRecהוא כלי תוכנה לשחזור נתונים לחוצץ קבצים עם ממשק משתמש גרפי. כמו PhotoRec,הוא אינו משחזר את שמות הקבצים המקוריים, אך הוא יכול לשחזר קבצים למחוק אפילו ממערכת קבצים פגומה.

Machine Translated by Google

פֶּרֶק

דו:

הַתקָנָה

2.1לינוקס: התקנה של חבילת הפצה

2.1.1 Arch Linux

,בתור שורשArch Linux. -במ-Extra repo זמיןTestDisk

```
pacman -S testdisk
```

2.1.2 CentOS

,בתור שורשCentOS. עבורEPEL זמינים במאגרTestDisk ו-QPhotoRec

```
יאם התקן epel-release יאם התקן
testdisk qphotorec
```

אם מאגר epelמושבת ב-CentOS בשלך, השתמש

```
yum install --enablerepo=epel testdisk qphotorec
```

2.1.3 ClearLinux

כדי להתקין את חבילת TestDisk ב-ClearLinux, לָרוּץ

```
sudo swupd bundle-add testdisk
```

2.1.4דביאן

Debian. זמין עבורTestDisk

בתור שורש,

```
update apt install testdisk
apt
```

Machine Translated by Google

פדורה2.1.5

זמין עבורTestDisk .Fedora

בתור שורש,

```
testdisk qphotorec התקןdnf
```

2.1.6 Fedora Copr

קופר היא מערכת בנייה אוטומטית עבור .Fedoraזה מספק את גרסת הפיתוח העדכנית ביותר. בתור שורש,

```
להתקיןgrenier/testdisk dnf אפשרdnf copr
testdisk qphotorec
```

ג'נטו2.1.7

זמין ב- .GentooTestDisk

```
app-admin/testdisk שאלsudo emerge --
```

2.1.8 openSUSE

```
testdisk photorec qphotorec התקןzypper רענוןzypper
```

אובונטו2.1.9

בתור שורש על אובונטו מַעֲרֶכֶת,

```
apt update apt install testdisk
```

Homebrew התקנה באמצעות2.2 macOS:

התקן -מbrew https://brew.shאם לא עשית זאת:

```
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/ install.sh)"
```

לאחר מכן, התקן testdisk

```
להתקין testdisk
```

Machine Translated by Google

2.3 קבצים בינאריים רשמיים

2.3.1 קבצים בינאריים רשמיים: יציב או ? WIP

בדרך כלל מומלץ להשתמש בגרסת הפיתוח (WIP=Work In Progress), מכיוון שתיקונים אינם מועברים לאחור. ניתן לשנות את ארכיון המספר פעמים בשבוע, אך לשמור על אותו שם. אם גרסה זו לא מתחילה, אתה תמיד יכול להשתמש בגרסה היציבה ולהזהיר את WIP-המפתח על הבעיה בגרסת הבטא.

2.3.2 התקנה של קבצים בינאריים רשמיים עבור Windows

- הורד את הארכיון (32 סיביות x86 או 64 סיביות (x64) מ- https://www.cgsecurity.org/wiki/TestDisk_Download
- חלץ את כל הקבצים כולל ספריות המשנה

2.3.3 התקנה של קבצים בינאריים רשמיים עבור macOS

הורד את הארכיון מאתר https://www.cgsecurity.org/wiki/TestDisk_Download

- macOS / Mac OS X Intel / OS X 64 סיביות (macOS >= 10.6)
- macOS / Mac OS X Intel / OS X 32 סיביות (macOS <= 10.14)
- Mac OS X PowerPC עבור Mac ישן מאוד (macOS <= 10.5)

חלץ את כל הקבצים כולל ספריות המשנה

2.3.4 התקנה של קבצים בינאריים רשמיים עבור לינוקס

הורד את הארכיון מאתר https://www.cgsecurity.org/wiki/TestDisk_Download כרגע יש לנו

- https://www.cgsecurity.org/testdisk-7.2.linux26-x86_64.tar.bz2 לגרסה היציבה האחרונה
- https://www.cgsecurity.org/testdisk-7.3-WIP.linux26-x86_64.tar.bz2 עבור גרסת הפיתוח

הארכיון מכיל קבצים בינאריים סטטיים עבור פלטפורמות אינטל x86_64) או i686). והם צריכים לעבוד כפי שהם בכל הפצת לינוקס עדכנית.

דחוס את הארכיון, אין צורך להיות root

```
tar xjf testdisk-7.3-WIP.linux26-x86_64.tar.bz2
```

רשום את הקבצים שלך (ls), ספרייה בשם testdisk-7.3-WIP צריכה נוצרה בספריית העבודה הנוכחית.

אזהרה: ייתכן שהקבצים הבינאריים המוכנים לשימוש של Linux לא יפרטו שמות קבצים נכונים ממערכות קבצים NTFS או exFAT. קבצים בינאריים אלה המסופקים cgsecurity.org-בהם קבצים בינאריים סטטיים. לרוע המזל, יישום iconv של GNU C Library משתמש במודולים משותפים הניתנים לטעינה כדי ליישם את ההמרות של Unicode. יש להשבית תמיכת iconv אחרת הקבצים הבינאריים יקרסו אם גרסת glibc-ההמקומית לא תואמת את גרסת glibc-ההמשמשת בעת ההידור.

Machine Translated by Google

Machine Translated by Google

פֶּרֶק

שְׁלוֹשָׁה

בנייה מהמקור

בניית קוד המקור שמורה בדרך כלל ל

- מפתחים שרוצים להוסיף תכונות חדשות
- מארזים המעוניינים ליצור ארכיון/חבילה להפצה
- משתמשים המשתמשים בפלטפורמה שעבורה אין קבצים בינאריים מוכנים לשימוש

3.1 סביבת קומפילציה

TestDisk משתמש במספר ספריות אם זמינות:

- libncurses - Required, TestDisk ו-PhotoRec משתמשים בממשק משתמש טקסט, ספריית Ncurses וקבצי פיתוח חייב להיות זמין.
- ספריית Ext2fs - אופציונלית, בשימוש על ידי TestDisk כדי לרשום קבצים ממחיצת ext2/ext3/ext4 ועל ידי PhotoRec כדי להיות מסוגלים לחצוב את החלל הפנוי ממחיצה ext2/ext3 במקום המחיצה כולה
- ספריית EWF - אופציונלי, TestDisk ו-PhotoRec משתמשים בה כדי לגשת לקבצי דחיסה של Expert Witness (למשל מקיף קבצים)
- Iconv - אופציונלי, משמש לטיפול בשמות קבצים של Unicode
- ספריית JPEG - אופציונלי, משמשת את PhotoRec לשיפור קצב שחזור JPEG
- ספריית NTFS - אופציונלי, בשימוש על ידי TestDisk לרשימת קבצים ממחיצת NTFS
- ספריית Reiserfs - אופציונלית, משמשת את TestDisk לרשימת קבצים ממחיצת reiserfs
- zlib library - אופציונלי, בשימוש על ידי PhotoRec כדי לשחרר דחיסה של תוכן gzipped
- ספריית Qt5 - אופציונלי, נדרש עבור QPhotoRec וכדי לעדכן את סקריפט התצורה.

3.1.1 לינוקס

- Debian/Ubuntu: apt-get install build-essential e2fslibs-dev libewf-dev libncurses5-dev uuid-dev zlib1g-dev qtbase5-dev qttools5-dev-tools pkg-config dh-autoreconf git libncursesw5-dev ntfs-3g-dev libjpeg-
- RHEL/CentOS 6 ואילך: yum התקן @buildsys-build desktop-file-utils e2fsprogs-devel libewf-devel libjpeg-devel libuuid-devel ncurses-devel ntfs-3g-devel qt-devel qt5-qtlibe-devel git

libjpeg-devel libuuid-devel ncurses-devel ntfs-3g-devel qt-devel qt5-qtbase-devel zlib-devel git

dnf התקנת @buildsys-build desktop-file-utils e2fsprogs-devel libewf-devel

Machine Translated by Google

3.1.2 macOS

Xcode התקן

```
xcode-select --install
```

התקן חליטה

```
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/ install.sh)"
```

brew באמצעותpkg-config, libjpeg-turbo ו-wget התקן

```
pkg-config libjpeg-turbo wget התקנתbrew
```

הורד את הספרייה המבוקשת (התאם את הגרסה)

```
download.tuxera.com/opensource/ntfs-3g_ntfsprogs-2017.3.23.tgz wget - N https://www.cgsecurity.org/testdisk-7.2.tar.bz2
wget -N http://prdownloads.sourceforge.net/e2fsprogs/e2fsprogs-1.46.2.tar.gz wget -N https://
```

שחרר וקומפיל אותם (החלף / User/kmasterבנתיב הנכון)

```
e2fsprogs-1.46.2 && ./configure cd &. make &. ntfs-3g_ntfsprogs-2017.3.23 && ./configure --disable-ntfs-3g --disable-nfconv && make && cd ..
tar xzf e2fsprogs-1.46.2.tar.gz tar xzf ntfs-3g_ntfsprogs-2017.3.23.tgz tar xzf testdisk-7.2.tar.bz2 cd

mkdir -p testdisk ../testdisk-7.2/configure --disable-qt \

Users/kmaster/ntfs-3g_ntfsprogs-2017.3.23/libntfs-3g/.libs/ \ --with-ntfs3g-includes=/Users/kmaster/ntfs-3g_ntfsprogs.3.231/7
ext2fs-lib=/Users/kmaster/e2fsprogs-1.46.2/lib \ --with-ext2fs-includes=/Users/kmaster/e2fsprogs-1.46.2/lib \ --with-ntfs3g-lib=/
\ --with-jpeg-lib=/usr/local/opt/jpeg-turbo/lib \ --with-jpeg-includes=/usr/local/opt/jpeg-turbo/include make /לכלול--with-

תקליטור..
```

3.1.3 Windows

cygwin

Cygwin https://cygwin.com/הוא אוסף גדול של כלים של GNUוקוד פתוח המספקים פונקציונליות דומה להפצה של לינוקס Windows-בהוא כולל את המהדר GCC. DLL (cygwin1.dll)מספק פונקציונליות משמעותית של POSIX API, פונקציות כאלה עשויות להידרש על ידי ספריות מסוימות שבהן TestDisk או PhotoRec יכולים להשתמש.

Machine Translated by Google

MinGW-w64

MinGW-w64 https://www.mingw-w64.org/ היא סביבת פיתוח תוכנה חינמית וקוד פתוח ליצירת יישומי Microsoft Windows. הוא מספק GCC עבור Windows 64 ו-23 סיביות.

3.2 סביבת קומפילציה צולבת

באמצעות לינוקס, ניתן ליצור קבצים בינאריים עבור Windows. שתי שרשרות כלים צולבות מהדרים זמינות תחת Fedora ליצירת קבצים בינאריים עבור Windows 32 ו-46 סיביות. כל החבילות הדרושות זמינות בכתובת

• יעד Cygwin של Windows
  – https://copr.fedorainfracloud.org/coprs/grenier/cygwin-testdisk/
  – https://copr.fedorainfracloud.org/coprs/yselkowitz/cygwin/
• יעד MinGW של Windows
  – https://copr.fedorainfracloud.org/coprs/grenier/mingw-testdisk/

testdisk, photorec ו-fidentify בינאריים רשמיים נוצרים באמצעות Cygwin, qphotorec באמצעות MinGW.

3.3 קומפילציה

3.3.1 הידור מארכיון המקורות

לאחר שהורדת את ארכיון המקור מ- https://www.cgsecurity.org/wiki/TestDisk_Download, לָרוּץ

```
cd testdisk-7.2 ./configure && make
tar xjf testdisk-7.2.tar.bz2
```

3.3.2 קומפילציה ממאגר git

```
שיבוט git https://git.cgsecurity.org/testdisk.git
```

אם כבר שיבטת את הפרויקט, כדי לעדכן את העותק המקומי שלך, הפעל את git pull מספריית testdisk.

```
config autoreconf --install -W all -I config ./configure make
cd testdisk mkdir
```

Machine Translated by Google

3.3.3הידור של גרסה סטטית

לאחר שהצלחת לבנות גרסה "רגילה", תוכל לנסות לבנות גרסה סטטית.

```
לעשות סטטי
```

מבנה סטטי היא גרסה מהודרת של תוכנית שקושרת סטטית נגד ספריות. בינארי סטטי אינו תלוי בזמינות הספרייה של המחשב עליו הוא פועל, בדרך כלל אתה יכול להעתיק את הבינארי הזה למחשב אחר וזה יעבוד. זה עדיין ספציפי לארכיטקטורה (כלומר CPU(ויכול להיות תלוי בליבה (גרסת מערכת ההפעלה), כך שניתן להשתמש בבינאריים סטטיים עבור יישומים ניידים. כדי שהבנייה תצליח, ייתכן שתצטרך להתקין גרסה סטטית של ספריות.

Machine Translated by Google

פֶּרֶק

ארבע

יצירת USBחי

אם אתה צריך לתקן מחשב שאינו מאתחל כהלכה, אתה יכול להעביר את ההארד-דיסק שלו למחשב עובד או להפעיל את המחשב ממפתח USBאו DVD.זה פתרון מאוחר יותר זה שיוצג כאן.

אתה צריך כונן הבזק מסוג USBהמכונה גם סטיק USB,כונן אצבע, כונן עט או כונן קפיצה שתוכל למחוק. שימו לב שאפשר גם להשתמש DVD-בריק.

הורד את "Image Live" Fedoraמ https://fedoraproject.org/fr/workstation/download/

4.1חלונות

- הורד והפעל את Rawrite32
- בחר את תמונת פדורה כתמונת מערכת הקבצים -אם קובץ התמונה אינו מוצג, ייתכן שיהיה עליך לשנות את אפשרויות בורר הקבצים או לשנות את סיומת התמונה
- בחר את מקל USB-הכמטרה
- בדוק שוב שאתה ממש ממש בטוח שאתה לא צריך אף אחד מהנתונים על מקל ה-USB!
- לחץ על כתוב לדיסק. . .
- המתן לסיום הפעולה,

4.2לינוקס (שורת פקודה)

- זהה את שם מחיצת כונן ה-USB
- בטל את טעינת כל המחיצות המותקנות מאותו התקן (החלף את / run/media/user/mountpointבנקודת הטעינה הנכונה)
- השתמש ב-dd כדי ליצור את ההעתקה (התאם את המקור והיעד)

```
lsblk umount /run/media/user/mountpoint sudo dd if=/path/to/image.iso of=/dev/sdX bs=8M status=progress oflag=direct
```

המתן עד שתסתיים הפקודה. אם אתה מקבל :ddדגל מצב לא חוקי: שגיאת 'התקדמות', גרסת ה-dd שלך לא תומכת באפשרות status=progressותצטרך להסיר אותה (ולא תראה התקדמות הכתיבה).

> אזהרה: הפקודה ddחזקה מאוד ויכולה להרוס את כל הנתונים הקיימים במכשיר שצוין. ודא לחלוטין את שם המכשיר לכתיבה ואל תקלד את שם המכשיר בטעות בעת שימוש ב-dd!

Machine Translated by Google

(GNOME) לינוקס4.3

שיטה זו מיועדת לאנשים המריצים לינוקס עם GNOME, Nautilus ו-GNOME Disk Utility מותקן. התקנה רגילה של Fedora, או התקנה רגילה של GNOME של הפצות רבות אחרות, אמורה להיות מסוגלת להשתמש בשיטה זו.
ב-Fedora, ודא שהחבילות nautilus ו-gnome-disk-utility מותקנות. כלים גרפיים דומים לכתיבה ישירה עשויים להיות זמינים עבור שולחנות עבודה אחרים.

- הורד תמונת פדורה, בחר מקל USB שאינו מכיל נתונים שאתה צריך, וחבר אותו
- הפעל את Nautilus (קבצים) - למשל, פתח את הסקירה הכללית על ידי לחיצה על מקש התחל/סופר, והקלד קבצים, ואז הקש על לְהַכנִיס
- מצא את התמונה שהורדת, לחץ עליה באמצעות לחצן העכבר הימני, עבור אל פתח עם, ולחץ על Disk Image Writer
- בדוק שוב שאתה ממש ממש בטוח שאתה לא צריך אף אחד מהנתונים על מקל ה-USB!
- בחר את מקל ה-USB השלך כיעד , ולחץ על התחל שחזור. . .
- המתן עד שהפעולה תסתיים, ולאחר מכן הפעל מחדש את המחשב שלך, ועשה כל מה שאתה צריך לעשות כדי לאתחל מאת מקל USB - לעתים קרובות זה יכלול לחיצה או החזקת F12, F2 או Del.

4.4 OS X

- פתח מסוף
- הפעל את רשימת דיסקתילים. זה יפרט את כל הדיסקים המחוברים למערכת, כמו /dev/rdisk1, /dev/rdisk2 וכן הלאה. זהה - בזהירות רבה! - איזה מהם מתאים למקל ה-USB השבו ברצונך להשתמש כיעד. להלן, נניח שזה היה / dev/rdisk2 - שנה את הפקודות בהתאם למקל שלך.
- הפעל את diskutil unmountDisk /dev/rdisk2
- הקלד dd if=, ואז גרור ושחרר את קובץ התמונה של פדורה לחלון הטרמינל - זה אמור לגרום לכך שמיקום מערכת הקבצים שלו יצורף לפקודה. כעת השלם את הפקודה עם of=/dev/rdisk2 bs=1m, אך אל תלחץ על Enter עדיין. אתה צריך לסיים עם משהו כמו Desktop-x86_64-20-1.iso of=/dev/rdisk2 bs=1m sudo dd if=/Volumes/Images/ Fedora-Live-
- בדוק שוב שיש לך את מספר הדיסק הנכון ואתה ממש ממש בטוח שאתה לא צריך אף אחד מהנתונים על מקל ה-USB!
- לחץ על Enter

4.5 החל ממקל ה-USB

חבר את מפתח ה-USB במחשב הפגום ואתחל את המחשב הזה, ועשה כל מה שאתה צריך לעשות כדי לאתחל ממקל USB - לעתים קרובות זה יכלול לחיצה או לחיצה ממושכת של F12, F2 או Del. אם אתה משתמש במחשב Mac, החזק למטה על מקש Alt/Option השמאלי כדי לגשת לתפריט האתחול - אתה אמור לראות לוגו של פדורה. לחץ על זה כדי לאתחל.

https://docs.fedoraproject.org/en-US/quick-docs/ יצירת ושימוש בהתקנה-חיה-תמונה/index.html עמוד זה של מקורי מקורי

Machine Translated by Google

פֶּרֶק

חָמֵשׁ

אחסון: האם אני יכול לתקן אותו או לשחזר ממנו נתונים?

ישנם 3סוגי אחסון:

• אחסון צמוד ישיר (DAS)או אחסון מקומי עבור דיסקים קשיחים המחוברים באמצעות

– IDE/PATA

- SATA/eSATA

– SAS

- Firewire

-מכשירים המחוברים באמצעות USB(דיסק חיצוני, מצלמה דיגיטלית, כונן אצבע, טלפון...) באחסון המוני USB מצב

• רשתות שטח אחסון (SAN)

-פרוטוקול סיבים תעלות (FCP)

-ערוץ סיבים על גבי Ethernet (FCoE)

-מיפוי של iSCSI, –SCSI על TCP/IP

• אחסון מחובר ברשת (NAS)

-שיתוף Windows (CIFS/SMB)

-מערכת קבצים ברשת (NFS)

-טלפון או מצלמה דיגיטלית במצב Media Transfer Protocol (MTP)(גם אם מחובר באמצעות USB)

TestDisk & PhotoRecיכולים לשחזר נתונים מאחסון NAS-ıDAS. עבור שרת NAS (QNAP, Synology...), הם צריכים לפעול על השרת עצמו או שצריך להעביר את הדיסקים למחשב המריץ לינוקס (לפעמים FreeBSD). TestDisk & PhotoRec יכולים לאחסן נתונים משוחזרים בכל אחסון זמין מהמחשב שלך. בעת שחזור קבצים שנמחקו, היזהר להימנע מכתיבת נתונים חדשים לאותה מחיצה שבה אוחסנו הקבצים.

Machine Translated by Google

Machine Translated by Google

פֶּרֶק

שֵׁשׁ

הפעלת הכלים

6.1תמונת דיסק

ניתן להשתמש TestDisk-בוב-ceRotohP על תמונת דיסק:

- קבצי גלם (.dd)
- Encase (.E01)
- קבצי Encase מפוצלים (.E01, E02. . .)

קבצי גלם מפוצלים אינם נתמכים. אין צורך בזכויות מנהל כדי להפעיל testdisk או photorec על תמונת דיסק.

דוגמאות:

- photorec image.dd כדי לגלף תמונת דיסק גולמית photorec image.E01
- לשחזור קבצים מתמונת Encase EWF
- צילום 'תמונה.???' אם תמונת Encase-המפוצלת למספר קבצים.

6.2הפעלת TestDisk, PhotoRec או QPhotoRec תחת Windows

לחץ פעמיים על קובץ ההפעלה (testdisk_win.exe, photorec_win.exe או qphotorec_win.exe) מחשבון בקבוצת המנהלים. זכויות מנהל נחוצות כדי לקבל גישה ברמה נמוכה לכל המדיה (דיסק קשיח, מפתח USB, כרטיס חכם וכו'). Windows UAC (Vista ואילך) יבקש ממך לאשר שברצונך להפעיל את קובץ ההפעלה עם זכויות מנהל.

הערה: Windows עשוי להסתיר סיומות קבצים. במקרה זה, לא תראה את file:.exe, אז לחץ פעמיים על photorec_win testdisk_win, או qphotorec_win.

הערה: אם אתה רואה את cygwin1.dll לא נמצא, c\\cygwin חסר, חלץ את כל הקבצים מהארכיון לפני הפעלת TestDisk או PhotoRec.

Machine Translated by Google

6.3הפעלת TestDisk, PhotoRecתחת לינוקס

אתה צריך להיות rootכדי להפעיל את TestDisk אוPhotoRec, כדי שהם יוכלו לגשת לכל הדיסקים שלך.

```
testdisk-7.2 sudo ./testdisk_static
cd
```

```
cd testdisk-7.2
sudo ./photorec_static
```

הערה: אם מכשיר Raid-השלך (כלומר, Intel raid) חסר, הפעל את "sudo dmraid -ay" כדי להפעיל אותו.

6.4הפעלת QPhotoRec תחתLinux X.org X11

QPhotoRec הוא יישום Qt5, הוא לא נשלח עם הקבצים הבינאריים הרשמיים של לינוקס www.cgsecurity.org-מאבל זה זמין ברוב הפצת לינוקס או ניתן להידור ממקור. כדי להפעיל אותו בטרמינל,

```
sudo qphotorec
```

6.5הפעלת QPhotoRec תחתLinux Wayland

כדי להפעיל את QPhotoRecבמסוף,

```
xhost+מקומי:
sudo qphotorec
```

6.6הפעלת TestDisk, PhotoRecתחת macOS

אם אינך root, TestDisk(כלומר testdisk-7.2/testdisk) או PhotoRecיפעילו את עצמם מחדש באמצעות sudoלאחר אישור מצדך.

אם לחשבון המנהל שלך אין סיסמה (סיסמה ריקה), עליך לתת למשתמש זה סיסמה לפני השימוש בפקודת sudo:

• בחר בתפריט Apple > System Preferences ולחץ על Accounts.

• לחץ על שנה סיסמה.

המסוף לא מציג את הסיסמה בזמן ההקלדה. אם תזין סיסמה שגויה או סיסמה ריקה, הפקודה לא מבוצעת ומסוף יבקש ממך לנסות שוב.

אם לא רשום דיסק בעת הפעלת TestDisk או PhotoRec, כנראה שזה נובע מהגנה על שלמות המערכת (SIP), בחר הגדרות מערכת ->פרטיות ואבטחה ->גישה מלאה לדיסק ->השתמש ב- +כדי להוסיף טרמינל (או PhotoRec-ו TestDiskעצמם)

Machine Translated by Google

6.7הפעלת Fidentify תחתWindows

Fidentifyבודק את כל הקבצים מתוך ספרייה עם אותן חתימות מאשר PhotoRec. זה שימושי לבדוק אם PhotoRecמסוגל לשחזר כמה סיומות קבצים/פורמטים מסוימים של קבצים. הפעל את cmd,שורת הפקודה של Windows. cd היא הפקודה לשנות ספרייה.

```
cd testdisk-7.2 fidentify_win.exe d:\directory
```

6.8הפעלת Fidentify תחת לינוקס או macOS

הפעל מסוף, עבור לספריית testdiskוהשתמש fidentify-בכדי לבדוק אם הקבצים הקיימים בספרייה מזוהים. זיהוי זה זהה ב-PhotoRec.

```
cd testdisk-7.2 ./fidentify_static /home/user/
```

Machine Translated by Google

Machine Translated by Google

פֶּרֶק

שבעה

תיקון מערכת קבצים

תיקון מערכת קבצים עשוי להיות עסק מסוכן שכן לפעמים הבעיה "מתוקנת" על ידי הסרת כל הקבצים הלא חוקיים. אז אם יש לך גישה לחלק מהקבצים שלך אבל לא לכולם, מומלץ לגבות את מה שאפשר לגשת לפני שתנסה לתקן את מערכת הקבצים.

7.1תיקון מערכות קבצים מ-Windows

Windowsיכול לקרוא ולכתוב קבצים ממערכת הקבצים FAT, exFAT ו-NTFS. הפקודה chkdsk משמשת לבדיקה ותיקון של מערכות קבצים. הפעל cmd (לחץ לחיצה ימנית על הפעל כמנהל)

```
chkdsk /fd:
```

7.2תיקון מערכות קבצים מ-xuniL

לינוקס יכולה לקרוא ולכתוב ממגוון גדול של מערכות קבצים. הפקודה הגנרית fsck משמשת להפעלת בדיקת מערכת קבצים. כדי לבדוק ולתקן אוטומטית את מערכת הקבצים ב-/dev/sda, הפעל כ-root

```
fsck -y /dev/sda1
```

fsckמתחיל פקודה ספציפית למערכת קבצים, למשל עבור ext4, הוא מפעיל את fsck.ext4. אם אתה צריך תיקון עדין, עליך לקרוא את דף ה-man של הפקודה הקשורה למערכת הקבצים שברצונך לתקן, כלומר man fsck.ext4. אם חסרים כמה קבצים או ספריות, זכור לבדוק את ספריית האבודים+נמצאו בשורש מערכת הקבצים הזו.

[illegible] Windowsשים לב שהוא מאפס את קובץ היומן NTFS,

7.3תיקון מערכות קבצים מ-macOS

כדי לבדוק כונן חיצוני,

```
sudo fsck /dev/disk1s1 רשימת
sudo diskutil
```

ייתכן שיהיה עליך לחזור על פקודת fsck מספר פעמים עד שלא תדווח שגיאה שנותרה.

אם אתה מקבל גודל צומת b-tree Invalid, אתה יכול לנסות

Machine Translated by Google


```
sudo fsck_hfs -r -d /dev/disk1s1
```

7.4תיקון מגזר האתחול של FAT32, exFAT ו-NTFS באמצעותTestDisk

מגזר האתחול הוא סקטור המכיל מידע הנדרש כדי לגשת לקבצים כלשהם ממערכת קבצים FAT, exFAT אוNTFS. למערכות הקבצים FAT32 ו-NTFS יש סקטור אתחול ראשי וגיבוי. אם סקטור האתחול הראשי פגום, מערכת הקבצים רשומה כגולמית או כבלתי ניתנת לקריאה. TestDisk מסוגל להשתמש בסקטור האתחול של הגיבוי כדי לתקן את סקטור האתחול הראשי:

- הפעל את TestDisk
- בחר את ההתקן המכיל את המחיצה (הימנע מאות כונן כמו :D)
- אשר את סוג טבלת המחיצות
- עבור לתפריט מתקדם
- בחר את המחיצה
- בחר אתחול

אם מגזר האתחול פגום, סקטור אתחול: רע יוצג. אם הגיבוי תקין, יופיע גם מגזר האתחול של גיבוי: . OK

- בחר BackupBS
- לאשר
- צא
- הפעל מחדש את המחשב

7.5תיקון מגזר האתחול FAT TestDisk:

הסקטור הראשון של מערכת קבצים FAT נקרא סקטור האתחול. הוא מכיל את מאפייני מערכת הקבצים הראשיים וכמה קוד קטן הנחוץ רק כדי להפעיל את המחשב ממחיצה זו. אם מגזר האתחול פגום, אי אפשר לגשת לנתונים שלך. Windows chkdsk או fsck Linux לא יכולים לתקן מערכת קבצים ללא סקטור אתחול חוקי, הם מחזירים הודעת שגיאה כמו Chkdsk אינו זמין עבור כונני RAW. למרבה המזל, TestDisk יכול למצוא את כל הפרמטרים שצריך להקליט בסקטור האתחול ולשכתב את הסקטור הזה, כך שניתן יהיה לבצע פעולות תיקון נוספות או גישה רגילה.

- הפעל את TestDisk
- בחר את ההתקן המכיל את המחיצה (הימנע מאות כונן כמו :D)
- אשר את סוג טבלת המחיצות
- עבור לתפריט מתקדם
- בחר את מחיצת ה-FAT
- בחר אתחול
- בחר RebuildBS
- בחר רשימה

אם testdisk מסוגל לרשום את הקבצים שלך, בחר

- צא מרשימת הקבצים
- בחר כתוב

Machine Translated by Google

- לאשר
- צא
- הפעל מחדש את המחשב

NTFS תיקון מגזר האתחול של7.6 TestDisk:

הסקטור הראשון של מערכת קבצים NTFSנקרא סקטור אתחול. הוא מכיל את מאפייני מערכת הקבצים הראשיים וכמה קוד קטן הנחוץ רק כדי להפעיל את המחשב ממחיצה זו. אם מגזר האתחול פגום, אי אפשר לגשת לנתונים שלך. Windows chkdskאו Linux fsckלא יכולים לתקן מערכת קבצים ללא סקטור אתחול חוקי, הם מחזירים הודעת שגיאה כמו Chkdskאינו זמין עבור כונני RAW. למרבה המזל, TestDiskיכול למצוא את כל הפרמטרים שצריך להקליט בסקטור האתחול ולשכתב את הסקטור הזה, כך שניתן יהיה לבצע פעולות תיקון נוספות או גישה רגילה.

- הפעל testdisk
- בחר את ההתקן המכיל את המחיצה (הימנע מאות כונן כמו :D)
- אשר את סוג טבלת המחיצות
- עבור לתפריט מתקדם
- בחר את מחיצת ה-SFTN
- בחר אתחול
- בחר RebuildBS
- בחר רשימה
- אם testdiskמסוגל לרשום את הקבצים שלך, בחר
- צא מרשימת הקבצים
- בחר כתוב
- לאשר
- צא

ext2/3/4 תיקון סופר בלוק של מערכת הקבצים7.7 TestDisk:

1024בתים לאחר תחילת מערכת הקבצים ext2/3/4יושב הסופרבלוק. הוא מכיל את מאפייני מערכת הקבצים העיקריים. עם סופר בלוק ראשי פגום, לא ניתן לעלות ולגשת לקבצים כרגיל. למרבה המזל עותקים של הבלוק הראשי פרוסים על מערכת הקבצים. ליתר דיוק, הם אינם עותק מדויק של הסופרבלוק הראשי, כל עותק מכיל מיקום משלו כדי למנוע בלבול בין עותקים למקור. TestDiskיכול לחפש בלוקים חלופיים.

- הפעל testdisk
- בחר את ההתקן המכיל את המחיצה
- אשר את סוג טבלת המחיצות
- עבור לתפריט מתקדם
- בחר את מחיצת לינוקס
- בחר SuperBlock

Machine Translated by Google


```
http://www.cgsecurity.org כלי לשחזור נתונים, אוגוסטTestDisk 7.1-WIP,
2016 Christophe GRENIER <grenier@cgsecurity.org>

dev/sda - 2000 GB / 1863 GiB - CHS 243201 255 63/ דיסק

חֲלוּקָה הַתחָלָה סוֹף גודל במגזרים

MS Data 2048 3907020799 3907018752 [/home2]
[/home2] superblock 229376, blocksize [home2]
[/home2] superblock 163840, blocksize=4096
blocksize=4096 [/home2] superblock 98304, blocksize=4096
superblock 0, blocksize=4096 [/home2] superblock 32768,
blocksize=4096 [/home2] superblock 4,695 סופרבלוק
884736, blocksize=4096 [/home2] superblock 1605632,
superblock 819200, blocksize=4096 [/home2] superblock
294912, blocksize=4096 [/home2]

blocksize device כדי לתקן את מערכת הקבצים באמצעות סופר בלוק חלופי, הפעל את
fsck.ext4 -p -b superblock -B

[ צא ]>
חזור לתפריט מתקדם
```

אם סופר בלוק 0רשום, זה אומר שהסופר בלוק הראשי נכון. אם הוא פגום, השורה הזו תחסר, השתמש במידע על גודל הבלוק הבא וגודל הבלוק כדי להפעיל .fsck

```
fsck.ext4 -p -b 32768 -B 4096 /dev/sda1
```

7.8תיקון כותרת נפח +HFS/HFS באמצעותTestDisk

כותרת אמצעי האחסון היא אתר 1024בתים לאחר תחילת מערכת הקבצים .+HFS/HFSאם הוא פגום, לא ניתן לגשת לקבצים כרגיל. TestDisk מסוגל להשתמש בכותרת נפח הגיבוי כדי לתקן את כותרת הנפח הראשי:

- הפעל את TestDisk
- בחר את ההתקן המכיל את המחיצה
- אשר את סוג טבלת המחיצות
- עבור לתפריט מתקדם
- בחר את המחיצה
- בחר SuperBlock

אם הבלוק הראשי פגום, כותרת Volume: Badתוצג. אם הגיבוי תקין, תופיע גם כותרת נפח הגיבוי: HFS+ Ok(או .(HFS Okבמקרה זה,

- בחר BackupBS
- לאשר
- צא

Machine Translated by Google

• הפעל מחדש את המחשב

7.9 תיקון נפח BitLocker

Repair-bde יכול לשחזר חלקים קריטיים של הכונן ולהציל נתונים הניתנים לשחזור כל עוד נעשה שימוש בסיסמת שחזור חוקית או מפתח שחזור כדי לפענח את הנתונים. ראה https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/ff829851(v=ws.11)

Machine Translated by Google

Machine Translated by Google

פֶּרֶק

שְׁמוֹנֶה

שחזור קבצים שנמחקו באמצעות TESTDISK

כאשר קובץ נמחק, הנתונים נשארים בדיסק. אלא אם כן נתונים חדשים החליפו את הקובץ האבוד שלך, TestDiskיכול בדרך כלל לשחזר אותו. זה אפשרי עבור

- FAT12/16/32
- exFAT
- NTFS
- ext2

עבור מערכות קבצים אחרות או אם עדיין חסרים קבצים מבוקשים, נסה את PhotoRec. PhotoRecהוא כלי עזר לשחזור קבצים מבוסס חתימה וייתכן שהוא יוכל לשחזר את הנתונים שלך כאשר שיטות אחרות נכשלו.

- אל תשתמש עוד במדיה (HDD, מפתח USB, . . .)שבה הנתונים המאוחסנים נמחקו עד לשחזור הנתונים התהליך הושלם.
- מומלץ מאוד TestDisk-שאו PhotoRecישחזרו קבצים על מדיית יעד אחרת, לפחות ב- מערכת קבצים אחרת.

למען אבטחה מרבית, TestDiskלא מנסה לבטל מחיקת קבצים אלא מאפשר לך להעתיק את הקבצים שנמחקו למחיצה או דיסק אחר. זכור, עליך להימנע מלכתוב דבר במערכת הקבצים שהחזיקה את הנתונים. אם תעשה זאת, קבצים שנמחקו עשויים להיחלף על ידי קבצים חדשים.

8.1 TestDisk: בטל מחיקת קובץ עבור FAT, exFAT, ext2

FATמשמש בעיקר בכרטיסי זיכרון ממצלמות דיגיטליות ובמפתחות USB. כאשר קובץ נמחק, שם הקובץ מסומן כמחוק ואזור הנתונים כבלתי מוקצה/חופשי, אך TestDiskיכול לקרוא את ערך הספרייה שנמחק ולמצוא היכן התחיל הקובץ. אם אזור הנתונים לא הוחלף על ידי קובץ חדש, הקובץ ניתן לשחזור.

exFATניתן למצוא בכרטיס זיכרון גדול, מפתחות USBגדולים ודיסק קשיח.

ext2היא מערכת קבצים של לינוקס. הוא הוחלף על ידי ext3 ו-ext4, כך שהוא לא נמצא לעתים קרובות כעת. עם ext3 ו-ext4, אפשר למצוא את שמות הקבצים שנמחקו אבל המיקום של הנתונים שנמחקו אינו זמין יותר, כך שגם אם ext3/ext4דומה ל-2txe, לא ניתן לשחזר קבצים שאבדו באמצעות TestDisk.

Machine Translated by Google

8.1.1הפעל את TestDisk

- הפעלת TestDisk, PhotoRec אוQPhotoRec תחתWindows
- הפעלת TestDisk, PhotoRec תחת לינוקס
- הפעלת TestDisk, PhotoRec תחתmacOS

8.1.2יצירת יומן

- בחר צור אלא אם יש לך סיבה להוסיף נתונים ליומן או אם אתה מפעיל TestDiskממדיה לקריאה בלבד ולא יכול ליצור אותו במקום אחר.
- הקש Enterכדי להמשיך.

8.1.3בחירת דיסק

כל הכוננים הקשיחים צריכים להיות מזוהים ולרשום בגודל הנכון על ידי .TestDisk

- השתמש במקשי החצים למעלה/למטה כדי לבחור את הכונן הקשיח שלך עם המחיצה/ים שאבדו.
- הקש Enterכדי להמשיך.

macOSאם זמין, השתמש במכשיר הגולמי / dev/rdisk*במקום / dev/disk*להעברת נתונים מהירה יותר.

8.1.4בחירת סוג טבלת מחיצות

TestDiskמציג את סוגי טבלת המחיצות.

- בחר את סוג טבלת המחיצות -בדרך כלל ערך ברירת המחדל הוא הנכון שכן TestDiskמזהה אוטומטית את סוג טבלת מחיצות.
- הקש Enterכדי להמשיך.

8.1.5התחל את תהליך ביטול המחיקה

- בחר מתקדם
- בחר את המחיצה שהחזיקה את הקבצים האבודים ובחר בטל מחיקה

8.1.6ביטול מחיקת הקובץ

נווט אל התיקיה שבה היו הקבצים שלך. קבצים וספריות שנמחקו מוצגים באדום.

- כדי לבטל מחיקה של קובץ, בחר את הקובץ לשחזור ולחץ על 'c'כדי להעתיק את הקובץ.
- כדי לשחזר ספרייה שנמחקה, בחר את הספרייה ולחץ על 'c'כדי לבטל את מחיקת הספרייה והתוכן שלה.

Machine Translated by Google

8.1.7בחר היכן יש לכתוב קבצים משוחזרים

בחר את היעד

8.1.8שחזור הקבצים הושלם

כשתחזיר את הקבצים שלך, השתמש ב- Quitכדי לצאת.

אם TestDiskלא הצליח למצוא את הנתונים שאבדו, נסה את PhotoRecבמקום זאת.

8.2 TestDisk: בטל מחיקת קובץ עבור NTFS

8.2.1הפעל את TestDisk

- הפעלת TestDisk, PhotoRec אוQPhotoRecתחת Windows
- הפעלת TestDisk, PhotoRecתחת לינוקס
- הפעלת TestDisk, PhotoRecתחת macOS

8.2.2יצירת יומן

- בחר צור אלא אם יש לך סיבה להוסיף נתונים ליומן או אם אתה מפעיל TestDiskממדיה לקריאה בלבד ולא יכול ליצור אותו במקום אחר.
- הקש Enterכדי להמשיך.

8.2.3בחירת דיסק

כל הכוננים הקשיחים צריכים להיות מזוהים ולרשום בגודל הנכון על ידי TestDisk.

- השתמש במקשי החצים למעלה/למטה כדי לבחור את הכונן הקשיח שלך עם המחיצה/ים שאבדו.
- הקש Enterכדי להמשיך.

אם macOSזמין, השתמש במכשיר הגולמי / *dev/rdiskבמקום / *dev/diskלהעברת נתונים מהירה יותר.

8.2.4בחירת סוג טבלת מחיצות

TestDiskמציג את סוגי טבלת המחיצות.

- בחר את סוג טבלת המחיצות -בדרך כלל ערך ברירת המחדל הוא הנכון שכן TestDiskמזהה אוטומטית את סוג טבלת מחיצות.
- הקש Enterכדי להמשיך.

Machine Translated by Google

8.2.5התחל את תהליך ביטול המחיקה

- בחר מתקדם
- בחר את המחיצה שהחזיקה את הקבצים האבודים ובחר בטל מחיקה

8.2.6ביטול מחיקה של קובץ NTFS

TestDiskסורק ערכי MFTלאיתור קבצים שנמחקו. מוצגת רשימה של קבצי NTFSשנמחקו שנמצאו על ידי TestDisk

- כדי לשחזר קובץ בודד, סמן את הקובץ ולחץ על 'c'(אותיות קטנות) כדי להעתיק אותו.
- כדי לשחזר מספר קבצים, העבר את הקובץ הראשון שברצונך לשחזר, לחץ על ':'כדי לבחור אותו, חזור על התהליך עבור קבצים אחרים, הקש על 'C'(אותיות רישיות) כדי להעתיק אותם

זה לא נראה בממשק אבל אפשר לסנן את התוצאות, לחץ על 'f'כדי להוסיף מסנן. ניתן להוסיף מספר מסננים. כדי לבטל את כל המסננים, הקש על 'r'(איפוס).

8.2.7בחר היכן יש לכתוב קבצים משוחזרים

בחר את היעד

8.2.8שחזור הקבצים הושלם

לאחר סיום שחזור קובץ ה-SFTN, בחר צא כדי לצאת.

אם TestDiskלא הצליח למצוא את הנתונים שאבדו, נסה את PhotoRecבמקום זאת.

Machine Translated by Google

פֶּרֶק

תֵּשַׁע

שחזור מחיצה שנמחקה באמצעות TESTDISK

כאשר מחיצה נמחקת או אם טבלת המחיצות פגומה, מערכות הקבצים נשארות בדיסק אך מיקומן אינו ידוע ולא ניתן לגשת לנתונים. TestDiskיכול לחפש מחיצות ולשכתב את טבלת המחיצות עם המחיצות שנבחרו על ידי המשתמש.

9.1הפעל testdisk

- הפעלת TestDisk, PhotoRec אוQPhotoRec תחת Windows
- הפעלת TestDisk, PhotoRec תחת לינוקס
- הפעלת TestDisk, PhotoRec תחת macOS

9.2יצירת יומן

- בחר צור אלא אם יש לך סיבה להוסיף נתונים ליומן או אם אתה מפעיל TestDisk ממדיה לקריאה בלבד ולא יכול ליצור אותו במקום אחר.
- הקש Enterכדי להמשיך.

אם בחרת ליצור את קובץ היומן, TestDisk מנסה ליצור קובץ בשם testdisk.log בספרייה הנוכחית.

הערה: משתמשי Windows, אם יש לך קשיים למצוא את הקובץ testdisk.log, בסייר הקבצים תחת תצוגה, בקבוצה הצג/הסתר, בחר בתיבת הסימון סיומות שם קובץ.

9.3בחירת דיסק

כל הכוננים הקשיחים צריכים להיות מזוהים ולרשום בגודל הנכון על ידי TestDisk.

- השתמש במקשי החצים למעלה/למטה כדי לבחור את הכונן הקשיח שלך עם המחיצה/ים שאבדו.
- הקש Enterכדי להמשיך.

הערה: - macOSאם זמין, השתמש במכשיר הגולמי / dev/rdisk*במקום / dev/disk*להעברת נתונים מהירה יותר.

Machine Translated by Google

> אזהרה: - macOSאם לא מופיע דיסק, בחר הגדרות מערכת <-פרטיות ואבטחה <-גישה מלאה לדיסק <-השתמש ב-+ כדי להוסיף טרמינל (או TestDiskעצמו)

> אזהרה: - Windowsאל תבחר :C:, Dאו אות כונן אחרת. זה חסר תועלת לחפש מחיצות בתוך מחיצה.

9.4בחירת סוג טבלת מחיצות

TestDiskמציג את סוגי טבלת המחיצות.

- בחר את סוג טבלת המחיצות -בדרך כלל ערך ברירת המחדל הוא הנכון שכן TestDiskמזהה אוטומטית את סוג טבלת מחיצות.
- הקש Enterכדי להמשיך.

הערה: עליך לבחור את סוג טבלת המחיצות שהיה בשימוש כאשר הייתה לך גישה לנתונים שלך.

9.5ניתוח טבלת המחיצות הנוכחית

- בחר ניתוח
- אשר באמצעות מקש Enter
- TestDisk יפרט את טבלת המחיצות הנוכחית.

אם מחיצה פגומה או ערך מחיצה פגום, הבעיה תופיע והמחיצה תופיע פעמיים. לדוגמה, אם אתה רואה "אתחול NTFSאו exFATלא חוקי" במחיצה (גודל המחיצה בסדר, המחיצה אינה חופפת למחיצה אחרת...) שאליו אתה רוצה לגשת, עדיף לתקן את הבעיה הזו NTFS (TestDisk: Repairing אתחול) לפני חיפוש מחיצות אחרות.

- אשר בחיפוש מהיר כדי להמשיך

9.6חיפוש מהיר למחיצות

TestDiskמציג את התוצאות הראשונות בזמן אמת. במידת הצורך, תוכל לבחור עצור כדי לבטל את החיפוש המהיר. TestDiskמפרט את כל המחיצות שהוא מצא. כדי לרשום את הקבצים של מערכת קבצים FAT, exFAT, NTFS, ext2/3/4, סמן מחיצה זו והקש Pהקש Qכדי לחזור לרשימת המחיצות.

Machine Translated by Google

9.7חפש מחיצות נוספות

אם מחיצה עדיין חסרה, בחר [חיפוש עמוק יותר]. זה יכול לקחת כמה שעות, אז אתה צריך להיות בטוח שהמחשב שלך לא יעבור למצב שינה (תכונת ניהול צריכת חשמל...)

9.8בחירת מחיצות

מחיצות הרשומות כ-D(מחיקה) לא ישוחזרו אם תאפשר להן לרשום כמוחקות. השתמש במקשי החצים כדי להחליף את המחיצות שברצונך לשחזר (בדוק את גודל המחיצה, רשום את תוכן הקובץ...) מ-D(מחק) ל-*(ניתן לאתחול), P(rimary) אוL(ogical). רק מחיצה אחת יכולה להיות רשומה בתור *(ניתנת לאתחול). זו לא בעיה אם מחיצה מסומנת כניתנת לאתחול בדיסק שלא תתחיל ממנו (למשל דיסק חיצוני) אבל חייבת להיות מחיצה ניתנת לאתחול בדיסק שממנו אתה רוצה להפעיל את המחשב.

לאחר שכל המחיצות שברצונך לשמור וכל המחיצות שברצונך לשחזר יסומנו כהלכה כלא נמחקו, המשך במסך הבא. עיין ברשימת המחיצות. אם כל המחיצות רשומות ורק במקרה זה, אשר -Writeבעם Enter, y וKO-. כעת, המחיצות רשומות בטבלת המחיצות.

אם נמצאה מחיצת FAT32 אוNTFS באמצעות סקטור האתחול של הגיבוי שלה, TestDiskיאפשר לך לשכתב את סקטור האתחול הראשי עם התוכן של סקטור האתחול של הגיבוי: כדי להעתיק את הגיבוי של סקטור האתחול מעל סקטור האתחול, בחר BS, Backupאמת באמצעות Enter, השתמש y-בכדי לאשר.

הפעל מחדש את המחשב.

Machine Translated by Google

פֶּרֶק

עֶשֶׂר

כיצד להפוך את המערכת לניתנת לאתחול מחדש

תבדוק את זה

- כל המחיצות מופיעות בטבלת המחיצות
- מחיצה עם מערכת ההפעלה של המחשב שלך מופיעה בתור *(ניתנת לאתחול)
- אתה יכול לרשום את הקבצים מהמחיצה הניתנת לאתחול

10.1 DOS - חלון 95/98

אם מערכת ההפעלה שלך לא מאתחלת, תוכל להתקין מחדש את קבצי המערכת באמצעות: sys c:.

10.2 Windows 2000/XP/2003

- הפעל את fixmbr ממסוף השחזור

```
fixmbr \Device\HardDisk0
```

אם עדיין יש לך את הבעיה,

- הפעל את fixboot כדי לתקן את סקטור האתחול של NTFS.
- בדוק את תוכן c:\boot.ini

10.3 Windows Vista/Windows 7/. . . , Windows Server 2008/. . .

הפעל את bootrec.exe /fixmbr ממסוף השחזור

- עבור טבלת המחיצות מדור קודם / PC Intel, בדוק את תוכן c:\boot.ini
- עבור EFI GPT, בדוק את הפלט של bcdedit /v. כדי לשנות את ההגדרות, השתמש בפקודה bcdedit /set.

הפעל את bootrec.exe /fixboot כדי לתקן את סקטור האתחול של NTFS.

אתחל את Windows במצב בטוח או DVD-משל Windows (לא DVD-המה-
ומחשב) https://support.microsoft.com/... windows-92c27cff-db89-8644-1ce4-b3e5e56fe234 כמו[2] ובחר

- פתרון בעיות
- אפשרויות מתקדמות

Machine Translated by Google

- שורת פקודה
- הפעל את chkdsk /fc: כדי לבדוק תיקון של מערכת הקבצים
- אם זה לא פותר את בעיית האתחול, נסה תיקון אתחול.

10.4 לינוקס/FreeBSD

- עדכן את / etc/fstab שלך כך שישקף את סדר המחיצות החדש.
- עדכן את תצורת ריבוי האתחול שלך
  – Lilo: /etc/lilo.conf
  – Grub: /boot/grub/grub.conf
  – Grub2: /etc/grub2-efi.cfg
- התקן מחדש את multiboot ברשומת האתחול הראשית.

```
device grub2-install device
lilo grub-install
```

Machine Translated by Google

פֶּרֶק

אַחַד עָשָׂר

שחזור קבצים שנמחקו באמצעות PHOTOREC

PhotoRec אינו משחזר את שמות הקבצים המקוריים או את מבנה הקבצים, אך הוא יכול לשחזר קבצים שאבדו אפילו ממערכת קבצים פגומה. PhotoRec הוא כלי לשחזור קבצים מבוסס חתימה (מחצב קבצים) וייתכן שהוא יוכל לשחזר את הנתונים שלך כאשר שיטות אחרות נכשלו.

זכור, עליך להימנע מלכתוב דבר במערכת הקבצים שהחזיקה את הנתונים. אם תעשה זאת, קבצים שנמחקו עשויים להיחלף על ידי קבצים חדשים.

11.1 הפעל את PhotoRec

- הפעלת TestDisk, PhotoRec או QPhotoRec תחת Windows
- הפעלת TestDisk, PhotoRec תחת לינוקס
- הפעלת TestDisk, PhotoRec תחת macOS

11.2 בחירת דיסק

מדיה זמינה מופיעה ברשימה. השתמש במקשי החצים למעלה/למטה כדי לבחור את הדיסק שמכיל את הקבצים האבודים.

- השתמש במקשי החצים למעלה/למטה כדי לבחור את הכונן הקשיח שלך עם המחיצה/ים שאבדו.
- הקש Enter כדי להמשיך.

רמז עבור macOS: אם זמין, השתמש במכשיר הגולמי /dev/rdisk* במקום /dev/disk* להעברת נתונים מהירה יותר.

אזהרה: macOS - אם לא מופיע דיסק, בחר הגדרות מערכת -> פרטיות ואבטחה -> גישה מלאה לדיסק -> השתמש ב-+ כדי להוסיף טרמינל (או PhotoRec עצמו)

11.3 בחירת מחיצת מקור

לִבחוֹר

- חפש לאחר בחירת המחיצה שמחזיקה את הקבצים האבודים כדי להתחיל את השחזור,
- אפשרויות לשינוי האפשרויות,
- File Opt כדי לשנות את רשימת סוגי הקבצים ששוחזרו על ידי PhotoRec.

Machine Translated by Google

11.4אפשרויות PhotoRec

• פרנואיד כברירת מחדל, קבצים משוחזרים מאומתים וקבצים לא חוקיים נדחים. הפעל את bruteforceאם אתה רוצה לשחזר קבצי JPEGמפוצלים יותר, שים לב שזו פעולה מאוד אינטנסיבית של מעבד, היא התחילה לאחר תהליך הסריקה הרגיל.

• אפשרות מצב המומחה מאפשרת למשתמש לאלץ את גודל הבלוק של מערכת הקבצים ואת ההיסט. לכל מערכת קבצים יש גודל בלוק משלו (כפולה של גודל הסקטור) והיסט 0)עבור NTFS, exFAT, ext2/3/4), ערכים אלו קבועים כאשר מערכת הקבצים נוצרה/פורמטה. כשעובדים על כל הדיסק (כלומר מחיצות מקוריות אבדו) או מחיצה שפורמטה מחדש, אם PhotoRecמצא מעט מאוד קבצים, אולי תרצה לנסות את הערך המינימלי PhotoRec-שמאפשר לך לבחור (זה גודל הסקטור) עבור גודל הבלוק 0)ישמש עבור ההיסט).

• אפשר את Keepקבצים פגומים כדי לשמור קבצים גם אם הם לא חוקיים בתקווה שעדיין ניתן להציל נתונים מקובץ לא חוקי באמצעות כלים אחרים.

• אפשר זיכרון נמוך אם למערכת שלך אין מספיק זיכרון והיא קורסת במהלך השחזור. זה עשוי להיות נחוץ עבור מערכות קבצים גדולות המפוצלות מאוד. אל תשתמש באפשרות זו אלא אם כן הכרחי.

11.5בחירת קבצים לשחזור

באפשר או השבת את השחזור של סוגי קבצים מסוימים, למשל, FileOpts-

```
[X]ריף RIFFאודיו/וידאו: wav, cdr, avi
...
[X] tif Tag Image File Formatוכמה פורמטים של קבצים גולמיים (pef/nef/dcr/sr2/cr2)
...
[X]ארכיון zip zipכולל MSOffice 2007-ו OpenOffice
```

כל הרשימה של פורמטי הקבצים ששוחזרו על ידי PhotoRecמכילה יותר מ-003 משפחות קבצים המייצגות יותר מ-084 סיומות קבצים.

> אזהרה: עבור פורמטים מסוימים של קבצים, PhotoRecיכול לקבוע את גודל הקובץ המקורי מכותרת הקובץ. עבור האחרים, PhotoRec מפסיקה להוסיף נתונים לקובץ שהוא משחזר כעת כאשר נמצאה כותרת קובץ חדשה. אז השבתת יותר מדי פורמטים של קבצים מובילה למספר רב של קבצים גדולים מדי.

11.6סוג מערכת הקבצים

לאחר בחירת מחיצה ואומתה באמצעות חיפוש, PhotoRecצריך לדעת כיצד מוקצים בלוקי הנתונים. אלא אם כן מדובר במערכת קבצים ext2/ext3/ext4, בבחר אחר.

Machine Translated by Google

11.7לחצוב את המחיצה או את החלל הלא מוקצה בלבד

PhotoRecיכול לחפש קבצים

- מכל המחיצה (שימושי אם מערכת הקבצים פגומה) או
- מהשטח הלא מוקצה בלבד (זמין עבור ext2/ext3/ext4, FAT12/FAT16/FAT32 ו-NTFS). עם האפשרות הזו רק קבצים שנמחקו משוחזרים.

11.8בחר היכן יש לכתוב קבצים משוחזרים

בחר את הספרייה שבה יש לכתוב את הקבצים המשוחזרים. השתמש במקשי החצים (למעלה, למטה, שמאלה, ימינה) כדי לנווט, אתה יכול גם להשתמש במקש Enterכדי להיכנס לספרייה.

- Dos/Windows/OS2: כדי לקבל את רשימת הכוננים C:, D:, E:) וכו'), השתמשו במקשי החצים כדי לבחור .., הקש על מקש Enter חזור עד שתוכל לבחור את הכונן לבחירתך. אמת עם Y esכאשר אתה מקבל את היעד הצפוי.
- לינוקס: מערכת קבצים מדיסק חיצוני עשויה להיות זמינה בתיקייה משנה / media, /mnt או / run/media. התקן את כונן היעד שלך במידת הצורך.
- macOS: מחיצות מדיסק חיצוני מותקנות בדרך כלל ב-/Volumes.

אזהרה: אל תאחסן את הקבצים המשוחזרים במערכת הקבצים המקור. אחרת נתונים שאבדו עלולים להידחק ולאבד באופן סופי.

אזהרה: הימנע מבחירת מערכת קבצים FAT32עבור היעד מכיוון שהיא אינה מטפלת בקבצים מעל 4 GB.

11.9השחזור מתבצע

מספר הקבצים המשוחזרים מתעדכן בזמן אמת.

- במהלך מעבר 0, PhotoRecמחפש את 10הקבצים הראשונים כדי לקבוע את גודל הבלוק. שלב זה נדלג בעת חיפוש קבצים מהשטח הלא מוקצה בלבד, נעשה שימוש בערך גודל הבלוק שנמצא במבנה מערכת הקבצים.
- במהלך מעבר 1ואילך, קבצים משוחזרים כולל כמה קבצים מקוטעים.

קבצים משוחזרים נכתבים בספריות משנה.-recup_dir.1, recup_dir.2. . . אפשר לגשת לקבצים גם אם השחזור לא הסתיים.

Machine Translated by Google

השחזור הושלם11.10

לאחר השלמת השחזור, יוצג סיכום. שים לב שאם תפריע לשחזור, בפעם הבאה PhotoRec-שיופעל מחדש תתבקש לחדש את השחזור.

- תמונות ממוזערות שנמצאות בתוך תמונות נשמרות כ-gpj.*t
- אם בחרת לשמור קבצים/שברי קבצים פגומים, שמות הקבצים שלהם יתחילו באות b(רוקן).
- ייתכן שהשבתת את הגנת האנטי-וירוס החיה שלך במהלך השחזור כדי לזרז את התהליך, אך מומלץ לסרוק את Windows: הקבצים המשוחזרים לאיתור וירוסים לפני פתיחתם - ייתכן PhotoRec-שביטלה מחיקה של מסמך נגוע או סוס טרויאני.
- רמז: כאשר מחפשים קובץ ספציפי. מיין את הקבצים המשוחזרים שלך לפי סיומת ו/או תאריך/שעה. PhotoRecמשתמש מידע זמן (מטא נתונים) כאשר זמין בכותרת הקובץ כדי להגדיר את זמן שינוי הקובץ.

הערה: - Windowsייתכן שיהיה עליך לקחת בעלות על התיקיות cc753659(v=ws.11) pro/windows-server-2008-R2-and -2008/ recup_dir.*: https://learn.microsoft.com/en-us/ previous-versions/windows/it-

---

הערה: - macOS / Linuxכדי לשנות את הבעלים של הקבצים, הפעל sudo chown -R username recup_dir.*

שם קובץ ותאריך11.11 PhotoRec:

ספריות חדשות, מקבצים של 500 קבצים בשם recup_dir.1, recup_dir.2. . . חדשים (קבצי האגודל אינם כלולים בספירה זו, וגם לא הקובץ report.xml). שם קובץ מתחיל באות ואחריה מספר (7 ספרות או יותר) ומסתיים, אם יש, בסיומת קובץ.

משמעות האות:

- f=קובץ
- b=שבור
- t=jpeg תמונה ממוזערת משובצת

המספר מחושב על ידי שימוש במיקום הקובץ פחות היסט המחיצה חלקי גודל הסקטור. עבור מערכות קבצים מסוימות כמו ext2/3/4, NTFS, exFAT, מספר זה עשוי להיות זהה למספר האשכול/בלוק המקורי כאשר גודל הבלוק שווה לגודל הסקטור.

באמצעות מידע מטא נתונים המוטבע בקובץ המשוחזר, ניתן לשנות את שם הקובץ כך שיכלול את כותרת התיעוד (לדוגמה, קבצי ppt Microsoft Office doc/xls/ או Acrobate pdf) כמו f0016741_Prudent_Engineering_Practice_for_Cryptographic_Protocols.pdf. recup_dir.1/

כברירת מחדל, זמני היצירה והשינוי של הקבצים מתאימים לזמן שחזור הנתונים. פורמט קובץ מסוים עשוי להטביע מידע על תאריך/שעה (כלומר תמונות jpg שצולמו על ידי מצלמה דיגיטלית, מסמכי Microsoft Office), PhotoRec ינסה לעשות בהם שימוש חוזר. בדרך זו, ייתכן שיהיה קל יותר למיין את הקבצים המשוחזרים. למטרות זיהוי פלילי, אל תסמוך על המידע הזה בצורה עיוורת: ייתכן שמידע התאריך/שעה יהיה כבוי בכמה שעות (אין או מידע שגוי על אזור הזמן) או שגוי לחלוטין (ייתכן שלשעון המכשיר המקורי הגדרת תאריך/שעה שגויה).

Machine Translated by Google

תואם שם הקובץ ומיקום הנתונים11.12 PhotoRec:

בואו ניקח דוגמה. PhotoRecשחזר קובץ וקרא לו f0017088.txt. קובץ זה מתחיל במגזר 17088 של מחיצה זו.

זה מגיע ממחיצת לינוקס שמתחילה במגזר 411648כפי שניתן לראות בממשק PhotoRec

```
2 P MS Data 411648 1460223 1048576 [/boot] [/boot]
```

הקובץ report.xmlמתעד את גודל הסקטור (מגזרי) ואת היסט המחיצה (img_offset)

```
<מקור>
<image_filename>/dev/sda</image_filename>
<sectorsize>512</sectorsize>
<device_model>CT500MX500SSD1</device_model>
<image_size>500107862016</image_size>
<נפח>
<byte_runs>
<byte_run offset='0' img_offset='210763776' len='536870912'/>
</byte_runs>
<block_size>4096</block_size>
</volume>
</source>
```

הפקודה testdisk -luמציגה את אותו מידע:

```
דיסק /dev/sda - 500 GB / 465 GiB - CHS 60801 255 63
גודל מגזר: 512
...

דיסק /dev/sda - 500 GB / 465 GiB - CHS 60801 255 63
חֲלוּקָה        התחלה   סוֹף   גודל במגזרים
1 P EFI מערכת   2048   411647   409600 [מחיצת מערכת EFI]
2 P MS Data   411648   1460223   1048576 [/boot] [/boot]
ext4 blocksize=4096 Large_file Sparse_SB שחזור
```

קיזוז של 210763776בתים הוא קיזוז של 411648סקטורים עבור גודל סקטור של 512בתים. קובץ זה מתחיל בסקטור 411648מתחילת הדיסק.

report.xmlמראה שהקובץ התחיל ב-238215912 בתים מתחילת הדיסק.

```
<fileobject>
<filename>f0017088.txt</filename>
<filesize>1024</filesize>
<byte_runs>
<byte_run offset='0' img_offset='219512832' len='4096'/>
</byte_runs>
</fileobject>
```

(219512832-210763776)/512=17088: קובץ זה מתחיל במגזר 17088של מחיצה זו.

עבור NTFS, exFAT, ext2/3/4, אם אתה צריך לקבל את האשכול או הבלוק הראשון של הקובץ, חלק את ההיסט באשכול גוֹדֶל. בדוגמה זו, האשכול הראשון הוא 2136: (219512832-210763776)/4096=2136 או אם אתה משתמש בשם הקובץ: 17088*512/4096=2136

Machine Translated by Google

Machine Translated by Google

פֶּרֶק

שְׁתֵּים עֶשְׂרֵה

יצירת חתימה מותאמת אישית עבור PHOTOREC

PhotoRecמזהה פורמטים רבים של קבצים. יש התייחסות ליותר מ-084 סיומות קבצים (כ-003 משפחות קבצים). לדוגמה, PhotoRec מסוגל לזהות את פורמט הקובץ JPEGוהוא יכול לשחזר קבצים שאבדו באמצעות פורמט זה, ללא קשר לסיומת הקובץ המקורית (jpg, jpeg, JPG...).

כדי לבדוק אם פורמט קובץ כבר מזוהה, אתה יכול

- עיין בפורמטים של הקבצים.
- שלח קובץ לדוגמה לבודק המקוון של PhotoRec.
- השתמש ב-fidentify בדוגמה של קובץ (ראה הפעלת Fidentifyתחת Windowsאו הפעלת Fidentifyתחת Linuxאו macOS)

```
[kmaster@adsl ~]$ fidentify /home/kmaster/src/testfiles/sample.pfi /home/kmaster/src/testfiles/sample.pfi: לא ידוע
```

במקרה זה, סוג הקובץ רשום כלא ידוע, כך ש-PhotoRec לא יכול לשחזר קובץ מסוג זה, לפחות כרגע. אנו נבדוק אם ניתן להוסיף חתימה מותאמת אישית עבורו.

אם במקום רשומה סיומת לא ידועה, PhotoRecמכירה את פורמט הקובץ הזה, היא עשויה לשחזר את הקובץ עם סיומת אחרת מהסיומת שאליה אתה רגיל.

12.1תחביר חתימה

הקובץ חייב להכיל הגדרת חתימה אחת בכל שורה. חתימה מורכבת מ

- שם הרחבה
- קיזוז החתימה
- חתימה או ערך קסם

ערך הקסם יכול להיות מורכב

- מחרוזות, למשל "נתונים". ניתן לבצע בריחה עם תווים מיוחדים כמו "0", "t", "r", "n", "b"או "\".
- נתונים הקסדצימליים, למשל 0x12, 0x1234, 0x123456. . . שים לב ש 0x12 0x34 0x56 ו-0x123456, 0x12, 0x34, 0x56- הם מקבילים.
-

מתעלמים ממפרידי רווח או פסיקים

על ידי שימוש בעורך הקסדצימלי, אתה יכול לראות שקובץ pfiמהדוגמה שלנו מתחיל במחרוזת ייחודית PhotoFiltre Image בהיסט 0.

Machine Translated by Google


```
00 00 00 00 00 |...............| ראש[kmaster@adsl ~]$ hexdump -C /home/kmaster/src/testfiles/sample.pfi |
03 40 06 00 00 b0 04 00 00 40 19 01 00 40 19 |e.@.......@...@.| 00000020 01 00 00 00 00 00 00 00 00 00
00000000 50 68 6f 74 6f 46 69 6c 74 72 65 20 49 6d 61 67 |PhotoFiltre Imag| 00000010 65
```

ניתן לכתוב את החתימה בשם

```
pfi 0 "PhotoFiltre Image"
```

או

```
"תמונה"pfi 0 "PhotoFiltre", 0x20,
```

או אם אתה מעדיף הקסדצימלי

```
pfi 0 0x50686f746f46696c74726520496d616765
```

מנקודת מבט של Fidentify/photorec, החתימות זהות.

> אזהרה: היזהר, hexdumpמציג תווים שאינם ניתנים להדפסה כנקודות. החתימה הבאה שגויה:
>
> ```
> pfi 0 "PhotoFiltre Image."
> ```
>
> חתימה זו באמצעות ערך הקסדצימלי במקום נקודה נכונה:
>
> ```
> pfi 0 "PhotoFiltre Image", 0x03
> ```

12.2מיקום הקובץ

PhotoRecמחפש את קובץ החתימה בשם

• Windows: photorec.sig בספריית USERPROFILEאו HOMEPATH, למשל C:\Documents and הגדרות\bob\ או C:\Users\bob.

• לינוקס ו-macOS: .photorec.sig בספריית HOME, למשל /home/bob/

• photorec.sig בספרייה הנוכחית

קובץ זה אינו קיים כברירת מחדל, עליך ליצור אחד. באמצעות עורך טקסט (למשל פנקס רשימות, vim. . .), צור את קובץ החתימה והוסף את החתימה שזיהית.

12.3בדוק את החתימה המותאמת אישית שלך עם fidentify

fidentifyכעת מזהה בצורה מושלמת את הקובץ

```
fidentify /home/kmaster/src/testfiles/sample.pfi /home/kmaster/src/testfiles/sample.pfi: pfi
[kmaster@adsl ~]$
```

אם fidentifyלא מזהה את החתימה,

• בדוק את החתימה שלך, ייתכן שהיא לא נכונה

Machine Translated by Google

• ודא שקובץ החתימה הוא קובץ טקסט אמיתי של ASCII. אסור להתחיל ב- EF BB BF (UTF-8 Byte Order Mark) או FF FE (UTF-16 LE BOM) לדוגמה.

• אמת את שם הקובץ של קובץ החתימה שלך

12.4 הפעל את PhotoRec

כעת אתה מוכן להשתמש ב-PhotoRec עם החתימה המותאמת אישית שלך כדי לשחזר את הקבצים שלך. אם קיים קובץ חתימה, PhotoRec ישתמש בו כברירת מחדל.

אזהרה: אם אתה משתמש ב-.photorec.sig בספריית HOME שלך , הזהיר שכאשר אתה מפעיל את photorec כ-root (כלומר באמצעות הפקודה sudo), photorec יחפש ב-/root/.photorec.sig, לא בבית המשתמש שלך מַדְרִיך. אז ייתכן שיהיה עליך להעתיק את הקובץ .gis.cerotohp תחילה.

12.5 שחזור קבצים משופר

כדי לשלוט בכל ההיבטים של השחזור (בדיקת תוכן הקובץ, בקרת גודל הקובץ, זיהוי כותרת תחתונה...), הדרך הטובה ביותר להוסיף חתימה, אם אתה מפתח, היא לשנות את PhotoRec עצמו.

תמיכה מסחרית זמינה גם מהסופר grenier@cgsecurity.org.

Machine Translated by Google

Machine Translated by Google

פֶּרֶק

שְׁלוֹשׁ עֶשְׂרֵה

שחזור סרטונים שאבדו מכרטיס זיכרון באמצעות PHOTOREC

בשל אופן הקלטת הסרטונים, כל הסרטונים שנוצרו על ידי מצלמה דיגיטלית כלשהי (כלומר Canon 5D Mark III, התמונות של TZ80 Panasonic DMC-במצב רצף) מפוצלים בכרטיס הזיכרון. תוכנת שחזור נתונים, כולל PhotoRec, צפו לקבצים לא מקוטעים.

אם כל הסרטונים (.mov / .mp4) ששוחזרו על ידי PhotoRec אינם ניתנים לקריאה, כנראה שאתה במקרה הזה. שימו לב פרק זה אינו נוגע להעתקים או קבצים שהורדו, רק קבצים שנכתבו על ידי מצלמה דיגיטלית כלשהי, לא על ידי המחשב שלכם.

בעת שימוש ב-PhotoRec, ב-FileOpts, בהפעל

```
[X] mov/mdat שחזר את mdat atom כקובץ נפרד
```

ובהמשך להתחיל את ההתאוששות.

אם אתה ממיין את הקבצים לפי שם, אתה אמור לראות שהשמות מתחלפים בין _ftyp.mov ל-_mdat.mov. אתה צריך לשרשר כל קובץ ftyp עם קובץ mdat:

• אם אתה משתמש ב-Windows, בהפעל cmd כדי להפעיל מסוף, השתמש cd directory_name בכדי להגיע למקום שבו נמצאים הקבצים שלך, והפעל

```
הקלד file2_ftyp.mov file1_mdat.mov > test.mov
```

אם אין לך הרשאות לכתוב לספרייה, לפני השימוש בפקודה type, קח בעלות על הספריות או הפעל cmd באמצעות קליק ימני, הפעל כמנהל.

• תחת macOS ו-Linux, הפעל מסוף/קונסולה, השתמש cd directory_name בכדי להגיע לאן שהקבצים שלך נמצאים, והפעל

```
cat file2_ftyp.mov file1_mdat.mov > test.mov
```

אם אין לך הרשאות לכתוב לספרייה, לפני השימוש בפקודה cat, שנה את הבעלות על הקבצים והספריות באמצעות recup_dir.* chown -R username:groupname

הפעל את הקובץ test.mov שהתקבל. אם זה עובד, אתה צריך לעשות את אותו הדבר עם כל זוג קבצים.

פתרון זה עובד רק עבור סרטונים שנכתבו בשני קטעים. סרטונים מ-GoPro HD2, Hero3-Black Edition, HERO4 Silver ממאוחסנים ביותר מ-2 קטעים, כך שדרושים פתרונות תוכנה מיוחדים לשחזור סרטונים כאלה. פרק זה אינו נוגע להעתקים או קבצים שהורדו, רק קבצים שנכתבו על ידי מצלמה דיגיטלית כלשהי, לא על ידי המחשב שלך.

הערה: התמונות של Panasonic DMC-TZ80 במצב רצף נשמרות כסרט. כדי לחלץ את התמונות מהסרט הזה, משתמשי macOS יכולים לייבא את הסרט לתמונות ולשמור כל פריים כתמונת סטילס בודדת.

Machine Translated by Google

Machine Translated by Google

פֶּרֶק

אַרְבַּע עֶשְׂרֵה

לאחר שימוש ב-PHOTOREC

בדרך כלל PhotoRec ו-QPhotoRec משחזרים הרבה קבצים אך ללא שמות הקבצים המקוריים, ייתכן שיהיה קשה לאתר את הקבצים שבהם אתה מעוניין.

14.1 מיון הקבצים לפי סיומת

14.1.1 שימוש בסקריפט powershell תחת Windows

https://github.com/lconte/Copy-PhotoRecFilesbyExtension.ps1

14.1.2 שימוש בסקריפט Python

Python מגיע מותקן מראש ברוב ההפצות של לינוקס ו-macOS. ניתן להתקין אותו גם תחת Windows. תוכנית Python sort-PhotorecRecoveredFiles

- ממיין את כל הקבצים לפי סיומות קבצים לתיקיות משלו.
- מגביל את מספר הקבצים/תיקיות על ידי יצירת תיקיות משנה אם חריגה ממספר מסוים. מספר הקובץ/תיקיה ניתן להתאים אישית.
- עבור כל "jpg": זה מכניס אותם לתיקיות משלהם בשנה (EXIF-Data). תוך שנה, פולדרים לכל אירוע נוצרים, למשל כל התמונות שצולמו בסוף שבוע או בחופשה אחת ממוינות בתיקייה אחת.

14.2 שינוי שמות של קבצים באמצעות exiftool

exiftool יכול להשתמש במטא-נתונים מכמה פורמטי קבצים פופולריים כדי לשנות את שמות הקבצים. כל ההפצות של לינוקס מגיעות עם חבילה עבור exiftool (קובץ:lrep- Image-ExifTool עבור Red Hat, CentOS ו-Fedora) אך חוץ מזה היא זמינה עבור Windows, Linux ו-macOS מאתר https://exiftool.org/

```
jpg/ exiftool -r -ext mov '-FileName<CreateDate' -d mov/%Y%m%d_%H%M%S%%-c.%%e mov/ exiftool -r -ext mp3 '-FileName<mp3/$
%Y%m/%%f.%%e doc/ exiftool -r -ext jpg '-FileName<DateTimeOriginal' -d sorted_jpg/%Y%m%d/%Y%m%d_%H%M%S%%-c. %%e
-r -ext avi '-FileName<DateTimeOriginal' -d avi/%Y%m%d_%H%M%S%%-c.%%e avi/ exiftool -r -ext doc '-FileName<CreateDate' -d doc/
%-c.%e ' mp3/f*.mp3 exiftool -r -ext mp3 '-FileName<mp3/${artist;} - ${Album;} - ${Title;}%-c.%e' -if 'not defined $ {אמן;}exiftool
$Title ו-$Title ne עקוב אחר והגדרת- ${Album;} - ${Track;} - ${Title;}

""' mp3/f*.mp3
```

(המשך בעמוד הבא)

Machine Translated by Google

(המשך מהעמוד הקודם)

```
מוגדרים לא$Album ו$Title ו-$Title ולא מוגדר$Track לא מוגדר'- ${Title;}%-c.%e' -if {;אמן}exiftool -r -ext mp3 '-FileName<mp3/$
"" ' mp3/f*.mp3
- $ {Title;}%-c.%e' -if 'not או$Title לא מוגדר)$Track and לא מוגדר'- ${Album;}%-c.%e' -if {;אמן}exiftool -r -ext mp3 '-FileName<mp3/$
FileName<ogg/${artist;} - ${Album;} - ${Track;} - ${Title;}%-c.%e ' ogg/f*.ogg exiftool -r -ext ogg '-FileName<ogg/${artist;} - ${Album;}
$Title eq "" )' mp3/f*.mp3 exiftool -r -ext ogg '-

$Title ו-$Title ne והגדר$Track הוגדר ogg/f*.ogg
לא מוגדר' אם- ${Title;}%-c.%e' - {;אמן}exiftool -r -ext ogg '-FileName<ogg/$
$Title ו$Title ne והגדר$Album לא מוגדר $Track ogg/f*.ogg
-ext m4p '-FileName<m4p/$ או$Title לא מוגדר)$Track and לא מוגדר'- ${Album;}%-c.%e' -if {;אמן}exiftool -r -ext ogg '-FileName<ogg/$
wma '-FileName<wma/${AlbumArtist;} - ${AlbumTitle;} - ${TrackNumber;}%- c.%e' wma/ {;אמן}$Title eq "" )' ogg/f*.ogg exiftool -r
sorted_tif/%Y%m%d/%Y%m%d_%H%M%S%%-c. %%e tif/ exiftool -r -ext ttf '-FileName<ttf/${FontName;}%-c.%e' ttf/ exiftool -r -ext
{Title;}%-c.%e' ps/ exiftool -r -ext rtf '-FileName<%f_${Title;}%-c.%e' rtf/ exiftool -r - ext tif '-FileName<DateTimeOriginal' -d
mkv/ exiftool -r -ext mp4 '-FileName< CreateDate' -d mp4/%Y%m%d_%H%M%S%%-c.%%e mp4/ exiftool -r -ext ps '-FileName<%f_$
- ${Album;} - ${Title;}%-c.%e' m4p/ exiftool -r -ext mkv '-FileName<%f_${Title;}%-c.%e'

exiftool -r -ext jpg '-FileName<IMG_${FileIndex}%-c.%e' recup_dir.*
```

14.3הסרת קבצים משוכפלים

תחת לינוקס, ניתן להשתמש בכדי להסיר קבצים משוכפלים-fslint

```
/usr/share/fslint/fslint/findup -d jpg/
```

Machine Translated by Google

פֶּרֶק

חֲמֵשׁ עֶשְׂרֵה

סטטוס חכם -ניטור בריאות הדיסק

חבילת smartmontoolsמכילה שתי תוכניות שירות (smartctl ו-smartd)לשליטה וניטור האחסון
מערכות המשתמשות במערכת הטכנולוגיה לניטור עצמי, ניתוח ודיווח (SMART)המובנית ברוב המודרני
דיסקים ATA/SATA, SCSI/SAS ו-NVMe. במקרים רבים, כלי עזר אלה יספקו אזהרה מתקדמת על השפלה וכשל של הדיסק.

חבילה זו מותקנת כברירת מחדל ברוב הפצת לינוקס. עבור Windows ו-macOS, יש בהתאמה א
gmd-ısetup.exe זמין מ- https://sourceforge.net/projects/smartmontools/files/smartmontools/

```
sudo smartctl -a /dev/sda
=== מדור תחילת המידע===
משפחת דוגמניות:    Western Digital Green
דגם מכשיר:    WDC WD20EZRX-00D8PB0
מספר סידורי: WD-WMC4M0875073 מזהה מכשיר LU WWN: 5 0014ee 058f9952c

גרסת קושחה: 80.00A80
קיבולת משתמש: 2,000,398,934,016בתים [2.00 TB]
גדלים של מגזר: 512בתים לוגיים, 4096בתים פיזיים
ההתקן הוא: במסד הנתונים smartctl [לפרטים השתמש: -P show]
גרסת ATAהיא: ACS-2 (עדכון קטן לא מצוין)
גרסת SATAהיא: SATA 3.0, 6.0 Gb/s (נוכחי: 6.0 Gb/s)
השעה המקומית היא: Tue Jul 19 11:18:12 2016 CEST תמיכת SMART זמינה - המכשיר כולל יכולת SMART.

תמיכת SMARTהיא: מופעלת

=== תחילת קריאה של קטע נתונים חכמים ===
תוצאת מבחן הערכה עצמית של בריאות כללית SMART: עבר
...
מספר גרסה של מבנה נתונים של תכונות SMART: 16
תכונות SMART ספציפיות לספק עם סף:
# ATTRIBUTE_NAME  דֶגֶל  ערך  הכי גרוע  סף  סוג  מעודכן  WHEN_FAILED
RAW_VALUE
5 Reallocated_Sector_Ct 0x0033 200 200 140  מראש נכשל תמיד  -  0
```

גם אם מצב הבריאות של SMART עבר, זה לא אומר שהדיסק תקין. עליך לבדוק גם את התכונה "Reallo-cated_Sector_Ct".

כאשר הכונן הקשיח מוצא שגיאת קריאה/כתיבה/אימות, הוא מסמן את המגזר הזה כ"מוקצה מחדש" ומעביר נתונים ל-
אזור שמור מיוחד (שטח פנוי). תהליך זה מכונה גם מיפוי מחדש, ומגזרים שהוקצו מחדש נקראים "מפות מחדש".
הערך הגולמי מייצג בדרך כלל ספירה של הסקטורים הגרועים שנמצאו והוספו מחדש. לפיכך, גבוה יותר
ערך התכונה, ככל שהכונן נאלץ להקצות מחדש יותר סקטורים. זה מאפשר לכונן עם סקטורים גרועים להמשיך
מִבצָע; עם זאת, כונן שבוצע בו הקצאות מחודשות יש סיכוי גבוה יותר להיכשל בעתיד הקרוב.
אמנם משמש בעיקר כמדד לתוחלת החיים של הכונן, אך מספר זה משפיע גם על הביצועים. בתור הספירה

Machine Translated by Google

מבין הסקטורים שהוקצו מחדש גדל, מהירות הקריאה/כתיבה נוטה להחמיר מכיוון שראש הכונן נאלץ לחפש לאזור השמור בכל פעם שניגשים למיפוי מחדש. אם מהירות הגישה הרציפה היא קריטית, ניתן לסמן באופן ידני את הסקטורים המחודשים כחסימות פגומות במערכת הקבצים על מנת למנוע את השימוש בהם.

אני ממליץ להחליף דיסק קשיח כאשר מופיעים הסקטורים הפגומים הראשונים.

Machine Translated by Google

פֶּרֶק

שֵׁשׁ עֶשְׂרֵה

שחזור נתונים מדיסק פגוםDDRESCUE:

סקטור רע הוא סקטור בכונן הדיסקים של המחשב שאינו נגיש או בלתי ניתן לכתיבה עקב נזק קבוע, כגון נזק פיזי למשטח הדיסק. זיכרון פלאש עשוי להיות גם "סקטורים גרועים" (גם אם מבחינה טכנית אין סקטור בזיכרון פלאש) עקב נזק קבוע כמו טרנזיסטורי זיכרון פלאש כושל.

במקום לעבוד ישירות על הדיסק הפגום, מומלץ ליצור עותק ולעבוד על השיבוט. שתי אפשרויות: ליצור תמונת דיסק (קובץ) או להחליף דיסק חדש/ריק.

בעת שיבוט דיסק לדיסק בריא, דיסק היעד יישאר בריא. אין דרך ליצור מחדש את התוכן החסר (תוכן שהיה מאוחסן בסקטור שכעת לא הצליח לקרוא), כך שאם הקובץ שעשה שימוש בסקטור זה "שוחזר", הוא ייפגע/יפגום.

> אזהרה: אל תפרמט מחדש דיסק אם ברצונך לשחזר את התוכן שלו. אין לעשות שימוש חוזר בדיסק עם סקטורים פגומים.
> התקנה מחדש של מערכת ההפעלה או פירמוט מחדש של המחיצה תסתיר במקרה הטוב את הבעיה לרגע.

ניתן למצוא ddrescueעבור Linux וmacOS. אם המחשב שלך משתמש במערכת הפעלה אחרת, אין בעיה, צור Linux Live USB! (ראה יצירת USBחי)

16.1 ddrescueבלינוקס

ddrescueזמין בכל הפצת לינוקס.

- CentOS: yum התקן ddrescue
- Debian/Ubuntu: apt התקנת gddrescue
- Fedora: dnf התקן ddrescue

השתמש lsblk-באו testdisk -lu כדי לזהות את כל הדיסקים.

16.2 ddrescue ב-macOS

כדי להתקין ddrescue:

- הקש Command+Space והקלד Terminal ולחץ על מקש enter/retur.
- הפעל באפליקציית טרמינל:

```
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/ install.sh)" brew install ddrescue
```

Machine Translated by Google

נַעֲשָׂה! כעת אתה יכול להשתמש ב-ddrescue. השתמש ברשימת diskutil כדי לקבל מידע על כל הדיסקים הזמינים וחלוקת המחיצות שלהם.

16.3 DDRescue: תמונת דיסק לקובץ

זו השיטה המומלצת למטרות משפטיות. אתה צריך מספיק מקום כדי לאחסן את הקובץ: אם אתה רוצה ליצור שיבוט של דיסק בנפח 1TB, אתה צריך לפחות 1TB פנוי במערכת קבצים. הימנע ממערכת קבצים FAT עבור היעד מכיוון שהם מוגבלים לקובץ של 4GB.

בדוגמה הבאה, תמונה בשם image_sdb.dd תיווצר מהדיסק השני /dev/sdb.

```
ddrescue /dev/sdb image_sdb.dd sdb.log
```

ניתן להשתמש בקובץ היומן sdb.log כדי להפעיל מחדש את השחזור. זה יכול לקחת כמה שעות עד כמה ימים כדי לשכפל דיסק עם הרבה סקטורים גרועים.

הערה: אם הגרסה שלך של ddrescue תומכת בהם, האפשרויות --check-on-error --reopen-on-error שימושיות כאשר ממשק הדיסק אינו יציב (משותף עם התקני USB) ועם --min-read-rate= 1M, ddrescue ישמור על האזורים האיטיים לסוף ההתאוששות.

16.4 DDRescue: העתקת דיסק לדיסק

דיסק היעד חייב להיות גדול לפחות כמו הדיסק המקורי. היזהר, שני דיסקים בעלי קיבולת זהה שהוכרזה מספקים שונים או לפעמים מדגמים שונים של אותו ספק יכולים להיות שונים מעט בגודלם (כמה 100 מגה-בייט).

כְּלוֹמַר. WD10EZRZ ו-WD10EZEX הם שני דגמים הנמכרים על ידי Western Digital כדגם 1TB, למעשה הראשון הוא 1,000,000 MB, השני 1,000,204 MB.

לפני שתתחיל, נתק את כל הדיסקים, התקן ה-USB, הקורא/כותב תקליטורים/DVD אין צורך: יש פחות סיכוי לשכתב את הדיסק הלא נכון.

```
ddrescue --force /dev/sdb /dev/sdc sdb.log
```

ניתן להשתמש בקובץ היומן sdb.log כדי להפעיל מחדש את השחזור.

16.5 ddrutility: הגבלת ddrescue לבלוק נתונים שהוקצה ל-SFTN

כאשר דיסק מכיל הרבה סקטורים גרועים, ייתכן שיהיה בטוח יותר להשתמש ב-ddrutility כדי להגביל את העותק לבלוק נתונים שהוקצה ממחיצת NTFS.

```
testdisk -lu /home/kmaster/data/data_for_testdisk/ntfs.dd TestDisk 7.1-WIP, כלי לשחזור
נתונים, אוגוסט Christophe GRENIER <grenier@cgsecurity.org> http://www.cgsecurity.org
2016 אנא המתן...


דיסק /dev/sdb - 130 MB / 124 MiB - CHS 16 255 63 (RO)
גודל מגזר: 512
```

(המשך בעמוד הבא)

(המשך מהעמוד הקודם)

```
דיסק /dev/sdb - 130 MB / 124 MiB - CHS 16 255 63 (RO)
מחיצה במגזרים                                   חֲלוּקָה
255456 [NTFS] 255487                            1 * HPFS - NTFS
                                                NTFS, blocksize=512
```

בדוגמה זו, מחיצת ה-SFTN הראשונה מתחילה במגזר 32וגודל המגזר הוא 512בתים.

```
ddru_ntfsbitmap /dev/sdb -i $((32 * 512)) sdb1_domain
ddrescue /dev/sdb sdb.dd sdb.log -m sdb1_domain
```

Machine Translated by Google

פֶּרֶק

שְׁבַע עֶשׂרֵה

ריצת SCRIPTED

TestDisk ו-PhotoRecיכולים לפעול באופן אוטומטי באמצעות הפקודות המובנות שלהם. קובץ סקריפט (כגון קבצי אצווה .dmc או .tab תחת MS-DOS/Windows, או מעטפת כלשהי תחת Linux) עשוי גם להיות מועיל.

17.1אוטומציה של שחזור באמצעות TestDisk

תַחבִּיר:

```
testdisk [/debug] [/log] [/logname file.log] /cmd [file.dd|file.e01|device] cmd
```

17.1.1כמה דוגמאות

```
debug /log /cmd partition.dd partition_none,geometry,H,32,analyze,list, advanced,boot,rebuildbs,list
testdisk /debug /log /cmd /dev/hda analyze,search testdisk /
```

17.1.2בחירת מכשיר

השתמש בשם ההתקן, למשל /dev/hda, /dev/hdb, /dev/sda.

עבור גישה למחיצה, ניתן גם להשתמש DOS dev/sda128/ עבור הדיסק הראשון, dev/sda129 / עבור השני וכן הלאה. . .
במירכאות בודדות, כלומר 'c:\input dir\image.dd' אם הנתיב או שם הקובץ מכילים רווחים. עבור קבצי Encase, אתה יכול להשתמש בקובץ. ה?? אם יש לך פחות מ-001 קבצים, אחרת השתמש בקובץ.???

17.1.3בחירת סוג מחיצה

• partition_i386

• partition_gpt

• partition_humax

• partition_mac

• partition_none

•מחיצה_שמש

• partition_xbox

• ask_type: המשתמש יתבקש עבור סוג המחיצה (חדש ב-9.6)

Machine Translated by Google

אם לא צוין או מתבקש סוג מחיצה, TestDiskיזהה אותו באופן אוטומטי.

17.1.4תפריט ראשי

- מתקדם
- לנתח
- למחוק
- גיאומטריה
- mbr_code
- אפשרויות
- רשימה

17.1.5תפריט ניתוח

גיבוי: שמור בקובץ backup.logאת מבנה המחיצות הנוכחי

- מספר: בחר מחיצה שנמצאה במהלך חיפוש מהיר או חיפוש עמוק יותר
- רשימה: רשימה של התוכן של המחיצה שנבחרה (הראשונה כברירת מחדל, חדשה ב-01.6)
- חיפוש: חיפוש עמוק יותר למחיצות נוספות
- לא לאשר, לכתוב
- לכתוב

17.1.6תפריט מתקדם

- סוג
- addpart: הוסף ערך מחיצה (לא נכתב לדיסק)
- אתחול: עבור מחיצת FAT12/FAT16, FAT32, exFAT ו-NTFS, עבור לתפריט הספציפי
- העתק: גיבוי המחיצה לקובץ image.dd(חדש ב-9.6)
- רשימה: רשום את תוכן המחיצה (חדש ב-01.6)
- רשימה, רקורסיבית: רשום את התוכן של המחיצה כולה (חדש ב-01.6)
- list,recursive,fullpathname: רשום את התוכן של המחיצה כולה עם שם הנתיב המלא (חדש ב-11.6)
- רשימה,קובץ עותק: רשום והעתק את כל הקבצים (חדש ב-1.7)
- superblock: חפש ב-2txe/ ext3 superblocks ואו עבור לתפריט HFS+ בהתאם למחיצה
- בטל מחיקה: עבור לתפריט ביטול המחיקה (FAT12/16/32, NTFS, exFAT, ext2)
- מספר: מספר המחיצה לבחירה

Machine Translated by Google

הוסף מחיצה

- PC Intel
  - צילינדר התנעה c,XX
  - ראש התחלה h,XX
  - מגזר מתחיל s,XX
  - צילינדר סיום C,XX
  - ראש מסתיים H,XX
  - מגזר סיום S,XX
  - סוג T,XX
- EFI GPT, Mac, XBoX
  - מגזר מתחיל s,XX
  - סקטור סיום s,XX
  - סוג T,XX
- Humax, Sun
  - צילינדר התנעה c,XX
  - צילינדר סיום C,XX
  - סוג T,XX

תפריט האתחול של FAT12/FAT16

- מזבלה
- רשימה (חדש ב-9.6)
- רשימה, רקורסיבית: רשום את התוכן של המחיצה כולה (חדש ב-01.6)
- list,recursive,fullpathname: רשום את התוכן של המחיצה כולה עם שם הנתיב המלא (חדש ב-11.6)
- בנייה מחדש
- תיקון שומן
- initroot

תפריט האתחול של FAT32

- מזבלה
- רשימה (חדש ב-9.6)
- רשימה, רקורסיבית: רשום את התוכן של המחיצה כולה (חדש ב-01.6)
- list,recursive,fullpathname: רשום את התוכן של המחיצה כולה עם שם הנתיב המלא (חדש ב-11.6)
- בנייה מחדש
- תיקון שומן
- שומן מקורי

Machine Translated by Google

- שומן גיבוי

תפריט בנייה מחדש של FAT

- רשימה
- רשימה, רקורסיבית: רשום את התוכן של המחיצה כולה (חדש ב-01.6)
- מזבלה
- לא לאשר, לכתוב
- לכתוב

תפריט האתחול של exFAT

- מזבלה
- originalexFAT
- backupexFAT

תפריט האתחול של NTFS

- בנייה מחדש
- מזבלה
- רשימה
- רשימה, רקורסיבית: רשום את התוכן של המחיצה כולה (חדש ב-01.6)
- list,recursive,fullpathname: רשום את התוכן של המחיצה כולה עם שם הנתיב המלא (חדש ב-11.6)
- originalntfs
- גיבוי nfs
- תיקון
- noconfirm,backupntfs
- לא לאשר,לתקן

תפריט ביטול מחיקה NTFS

- allundelete (חדש ב-1.7): רשום ושחזר את כל הקבצים שנמחקו. אזהרה: מאחסן אותם בספרייה המקומית הנוכחית.

תפריט בנייה מחדש של NTFS

- רשימה
- רשימה, רקורסיבית: רשום את התוכן של המחיצה כולה (חדש ב-01.6)
- list,recursive,fullpathname: רשום את התוכן של המחיצה כולה עם שם הנתיב המלא (חדש ב-11.6)
- מזבלה
- לא לאשר, לכתוב
- לכתוב

Machine Translated by Google

HFS+ superblock תפריט

- מזבלה
- originalhfsp
- backuphfsp

17.1.7תפריט גיאומטריה

- מספר צילינדרים C,
- מספר ראשים,H
- מספר מגזרים,S
- גודל מגזר N,

17.1.8אפשרויות

- מזבלה
- nodump
- יישור
- noalign
- מומחה
- ללא מומחה

17.2אוטומציה של שחזור באמצעות PhotoRec

```
photorec [/debug] [/log] [/logname file.log][/d recup_dir] [/cmd <device> <command>]
```

תחביר כללי:

הפעל את מצב ניפוי באגים?/debug:

הפעל רישום (קובץ יומן בשם photorec.log ייווצר/ יצורף אליו במצב העבודה הנוכחי • /log:
מַדרִיך

היומן ייכתב file.log-לבמקום photorec.log • /logname file.log:

ציין ספרייה שבה יש לאחסן את הקבצים המשוחזרים. זה צריך להיות במכשיר שונה מזה שאתה מתאושש ממנו. /d recup_dir:
PhotoRecתוסיף סיומת מספרית לנתיב שצוין, החל ב-"1." -ותגדיל את המספר הזה כל עוד ספרייה בשם זה כבר קיימת.

מציג את קטע הפקודה עבור הפעלת סקריפט? /cmd:

המכשיר (או קובץ התמונה) ממנו יש לשחזר (רמז: השתמש במירכאה בודדת אם קובץ התמונה מכיל רווחים) • <device>:

רשימת הפקודות (ראה להלן) • <command>:

Machine Translated by Google

17.2.1כמה דוגמאות לשחזור נתונים באמצעות PhotoRec

שחזור מהמחיצה השנייה של כונני IDE i386 שהמשתמש בוחר

```
photorec /debug /log /cmd /dev/hdb בחר,683i_noititrap,חפש
```

התאושש מכונני IDE-הראשונים מחיצת i386 #5, והמשתמשת ב-ext3/ext4/2txe

```
photorec /debug /log /cmd /dev/hda partition_i386,options,mode_ext2,5,search
```

שחזר מקובץ תמונת דיסק נתון בשם disk.dmp שיש לו רק מחיצת ext4 בודדת (או חלק ממנה) שחזר את כל סוגי הקבצים הידועים ל-PhotoRec ל-mnt/recover/disk./

```
photorec /debug /log /d /mnt/recover/disk /cmd disk.dmp options,mode_ext2,\ fileopt,everything,enable,search
```

אותו דבר ללא איתור באגים ויומן- אבל שחזר רק *.jpg ו-*.gif

```
photorec /d /mnt/recover/disk /cmd disk.dmp options,mode_ext2,fileopt,everything,disable,  \jpg,enable,gif,enable,search
```

שחזר jpg מהשטח הפנוי של המחיצה הראשונה

```
photorec /cmd /dev/hda fileopt,everything,disable,jpg,enable,freespace, search
```

שחזר את כל הקבצים משטח פנוי מכל מחיצה כפי שזוהה על ידי TestDisk

```
PARENT=pwd DEVICE=/dev/sda testdisk -l $DEVICE | tee testdisk.log | \

egrep "[[:digit:]][[:space:]][P,E,L,D,*][[:space:]].+([[:space:]]+[[:digit: ]]+){3}" | \ לחתוך -d\ 2 -f בזמן קריאת PARTITION לעשות

mkdir $PARTITION && cd $PARTITION && xterm -e photorec /log /debug /d ./ /cmd $DEVICE freespace, $PARTITION,חיפוש CD $PARENT נעשה
```

17.2.2רשימת פקודות

למטה תמצא רשימה של אפשרויות פקודה זמינות, מקובצות לפי קטגוריות. עדיף להשתמש בהם לפי הסדר שהם מוזכרים כאן. יש להפריד בין אפשרויות אלה בפסיק. ניתן להשתמש ישירות בבחירת סוג המחיצה ובאפשרויות מהתפריט הראשי.

Machine Translated by Google

בחירת סוג מחיצה17.2.3 PhotoRec -

• partition_i386
• partition_gpt
• partition_humax
• partition_mac
• partition_none
מחיצה_שמש•
• partition_xbox
המשתמש יתבקש עבור סוג המחיצה• ask_type:

אם לא צוין סוג מחיצה, היא מזוהה אוטומטית.

תפריט ראשי17.2.4 PhotoRec -

• שנה סוגי קבצים כדי לשחזר• fileopt:
• השימוש PhotoRec-בהופך לאינטראקטיבי• inter:
• אפשרויות•
• מספר: מספר המחיצה לבחירה•
• כפה על גודל הבלוק -ואחריו גודל הבלוק בבתים.• blocksize:
• גיאומטריה•
• קבצים ישוחזרו מכל המחיצה או רק מהשטח הפנוי (חדש ב• wholespace / freespace : 6.10)
• חורצים את הקבוצה שמספרה עוקב (חדש ב-01.6)• ext2_group:
• חצב את הקבוצה שהאינוד הבא שלה שייך (חדש ב-01.6)• ext2_inode:
• חיפוש: התחל את השחזור•

fileopt תפריט17.2.5 PhotoRec -

• הכל, אפשר: השתמש בערכים כברירת מחדל (עשויים להיות שונים מהערכים השמורים, חדש ב-9.6)
• הכל, השבת: רוקן את רשימת פורמטי הקבצים לאיתור (חדש ב-9.6)
• יחפש jpg• jpg,enable:
• לא יחפש jpg• jpg,disable:

אתה יכול להשתמש באותו תחביר עבור כל פורמטי הקבצים.

Machine Translated by Google

תפריט אפשרויות17.2.6 PhotoRec -

כדי להשתמש בכל דבר מתפריט האפשרויות, עליך לציין תחילה את מילת המפתח "אפשרויות".

- מומחה
- keep_corrupted_file_no (חדש ב-01.6)
- keep_corrupted_file
- paranoid_no / paranoid / paranoid_bf (חדש ב-01.6)
- lowmem
- mode_ext2

17.3 Windows UAC

אם אתה מפעיל את TestDisk ו-PhotoRec, בקרת חשבון משתמש של Windows ישאל "האם אתה רוצה שהתוכנית הבאה ממוציא לאור לא ידוע תשנה למחשב זה?" (או משהו דומה). מכיוון שאין צורך בזכויות מנהל עבור תמונות דיסק, ייתכן שתרצה להימנע מהנחיית UAC זו עם משתנה הסביבה __COMPAT_LAYER.
דוגמָה:

```
cmd image.dd חיפוש=REYAL_TAPMOC__ הגדר
RunAsInvoker photorec_win.exe /
```

Machine Translated by Google

פֶּרֶק

שְׁמוֹנֶה עֶשְׂרֵה

במבחנים דיגיטליים דיגיטליים משפטיים שונים TESTDISK ו-PHOTOREC מקרים

PhotoRecנחשב לאחד מכלי השירות הטובים ביותר לגילוף קבצים מכמה סיבות:

•תמיכה בפורמט קבצים: PhotoRecמסוגלת לשחזר מגוון רחב של סוגי קבצים, כולל תמונות, סרטונים, מסמכים וקובצי מוזיקה. זה יכול גם לשחזר קבצים ממערכות קבצים שונות, כולל ext3/ext4./2txe-וNTFS, exFAT, FAT

•יציבות: PhotoRecמסוגלת לשחזר קבצים גם אם מערכת הקבצים פגומה קשות או שהתקן האחסון עבר פורמט מחדש. זה יכול גם לשחזר קבצים שנמחקו או אבדו עקב עיצוב או שגיאות אחרות.

•גמישות: PhotoRecהוא כלי שורת פקודה, המעניק למשתמשים יותר שליטה וגמישות באופן שבו הם משחזרים קבצים. הוא כולל גם ממשק משתמש גרפי בשם QPhotoRec,המקל על משתמשים שפחות מכירים את ממשק שורת הפקודה.

•קוד פתוח: PhotoRecהיא תוכנת קוד פתוח. זה אומר שמשתמשים יכולים לראות את הקוד, לבצע שינויים ולהגדיר מחווה לפיתוח התוכנה.

•חינם: PhotoRecהוא חינמי לחלוטין לשימוש, מה שהופך אותו לנגיש למגוון רחב של משתמשים וארגונים.

כל הגורמים הללו הופכים את PhotoRecלכלי עזר רב עוצמה ורב-תכליתי לגילוף קבצים שניתן להשתמש בו כדי לשחזר מגוון רחב של קבצים מהתקני אחסון שונים.

תוכנית Computer Forensics Tool Testing (CFTT) היא תוכנית המנוהלת על ידי המכון הלאומי לתקנים וטכנולוגיה (NIST), שהיא סוכנות פדרלית בארה"ב המספקת תקנים טכניים והנחיות למגוון תעשיות וארגונים, כולל מדע משפטי. PhotoRecהוערך על ידי CFTT-הבשנת 2014למטרת גילוף קבצים משפטיים. PhotoRec-להיו התוצאות הטובות ביותר ;-)

ראוי לציין שבעוד Photorec-שהוא כלי בשימוש נרחב בחקירות משפטיות, הוא לא היחיד, וייתכן שהוא לא הטוב ביותר עבור מקרים מסוימים. כלים אחרים עשויים להתאים יותר לסוגים ספציפיים של חקירות או לסוגים ספציפיים של אמצעי אחסון. בחירת הכלי המתאים תהיה תלויה בצרכים הספציפיים של החקירה ובמומחיות הטכנית של החוקר המשפטי.

כדי ללמוד להשתמש TestDisk-בוב-ceRotohP, מקרי בדיקה שונים זמינים לתרגול בתנאים בטוחים.

18.1 DFTT: בטל מחיקת קבצים ממערכת קבצים FAT16

הורד את מערכת הקבצים הקטנה FATארכיון תמונות וחלץ את כל הקבצים. תמונת בדיקה זו היא מערכת קבצים של FAT16 6MBעם שישה קבצים שנמחקו ושתי ספריות שנמחקו. הקבצים נעים בין קבצי אשכול בודדים לשברים מרובים.

כדי לבטל את המחיקה של כל הקבצים באופן ידני,

•הפעל את testdisk 6-fat-undel.dd

•בחר המשך.

Machine Translated by Google

•מדיה לא מחולקת מזוהה באופן אוטומטי, הקש Enterכדי לאשר.

•בחר בטל מחיקה.

כל הקבצים והספריות נמחקים, הם רשומים באדום.

•הקש 'a'כדי לבחור את כל הקבצים.

הקבצים והספריות שנבחרו רשומים כעת בירוק ובקידומת '*'או '>'עבור הקובץ המסומן הנוכחי.

•הקש על 'C'(אותיות גדולות) כדי להעתיק את כל הקבצים והספריות שנבחרו.

•בחר יעד להעתקת כל הקבצים: השתמש במקשי החצים (למעלה, למטה, שמאלה, ימינה) כדי לנווט, אתה יכול גם להשתמש מקש enterכדי להיכנס לספרייה.

•לחץ על 'C'כאשר היעד נכון.

כל הקבצים מועתקים.

•הקש על 'q'כדי לצאת

•בחר [צא] עד שתצא מכל התפריטים

שמות הקבצים הרגילים עבור מערכת קבצים FATמורכבים מ-8 תווים עבור השם ו-3 עבור הסיומת. כאשר קובץ נמחק, התו הראשון של שם הקובץ מוחלף. TestDiskמייצג את התו האבוד באמצעות קו תחתון _(למשל _RAG1.DATבמקום FRAG1.DAT) אם קיים שם קובץ ארוך 8 <(תווים), הוא ישמש במקום זאת. היתרון הוא שניתן להציג את כל שם הקובץ (למשל מידע על נפח מערכת)

כל הקבצים משוחזרים בהצלחה מלבד 3הקבצים המפוצלים. הגודל של 3הקבצים האלה נכון אבל התוכן שגוי. כאשר קובץ נמחק, הרשימה המקושרת שנוצרה על ידי מספרי האשכולות המשמשים את הקובץ מסומנים כפנויים בטבלאות FAT. TestDiskמניח שאין פיצול אבל זה לא המקרה כאן.

18.2 DFTT: בטל מחיקת קבצים ממערכת קבצים NTFS

הורד את מערכת הקבצים הקטנה NTFSארכיון תמונות וחלץ את כל הקבצים. תמונת בדיקה זו היא מערכת קבצים NTFSשל 6MBעם שמונה קבצים שנמחקו, שתי ספריות שנמחקו וזרם נתונים חלופי שנמחק. הקבצים נעים בין קבצי תושב, קבצי אשכול בודד ופרגמנטים מרובים. שום מבני נתונים לא שונו בתהליך זה כדי לסכל התאוששות. הם נוצרו ב-Windows XP, בנמחקו XP-ובהצטלמו בלינוקס.

כדי לבטל את המחיקה של כל הקבצים באופן ידני,

•הפעל את testdisk 7-ntfs-undel.dd

•בחר המשך.

•מדיה לא מחולקת מזוהה באופן אוטומטי, הקש Enterכדי לאשר.

•בחר בטל מחיקה.

TestDiskמפרט את כל הקבצים שאבדו בהצלחה. זרם הנתונים החלופי רשום כ-./mult1.dat:ADS, זרמים חלופיים אינם רשומים בסייר Windows,וגודלם אינו כלול בגודל הקובץ. תוכנה זדונית השתמשה בזרמי נתונים חלופיים כדי להסתיר קוד. כתוצאה מכך, סורקי תוכנות זדוניות וכלים מיוחדים אחרים בודקים כעת זרמי נתונים חלופיים. מנתח פורנזי צריך גם לחפש אותם מכיוון שהם עשויים לשמש להסתרת מסמכים.

•הקש על 'C'(אותיות גדולות) כדי להעתיק את כל הקבצים והספריות שנבחרו.

•בחר יעד להעתקת כל הקבצים: השתמש במקשי החצים (למעלה, למטה, שמאלה, ימינה) כדי לנווט, אתה יכול גם להשתמש מקש enterכדי להיכנס לספרייה.

•לחץ על 'C'כאשר היעד נכון.

כל הקבצים מועתקים.

•הקש על 'q'כדי לצאת

Machine Translated by Google

• בחר [צא] עד שתצא מכל התפריטים

18.3 אתגר DFRWS 2006 לזיהוי פלילי

DFRWS 2006 Forensics Challenge הוא אתגר גילוף נתונים. אפשר להשתמש PhotoRec-בכדי לשחזר את רוב הקבצים:

• הפעל את photorec dfrws-2006-challenge.raw
• בחר המשך
• תפריט כניסות לאפשרויות
• הגדר "פרנואיד : כן (כוח גס מופעל)"
• הגדר "שמור קבצים פגומים: כן"
• השתמש "Quit"-בכדי לחזור לתפריט הראשי
• בחר חיפוש
• אשר את סוג מערכת הקבצים "[אחר]"
• השתמש במקש 'C' כדי לאשר את היעד של הקבצים המשוחזרים (ספרייה נוכחית)
• המתן לסיום השחזור
• צא

כל השלבים האלה יכולים להיות גם אוטומטיים בפקודה אחת:

```
photorec /log /d recup_dir /cmd dfrws-2006-challenge.raw options,paranoid_bf,keep_ corrupted_file,search
```

הקובץ לניתוח הכיל 32 קבצים (לא כולל את הקבצים המוטבעים, כגון תמונות במסמכי Word או הקבצים בתוך קובצי ZIP). 32 הקבצים שימשו ליצירת 22 תרחישים שונים. כל תרחיש תוכנן לבדוק מצב ספציפי שעלול להתרחש במערכת קבצים אמיתית.

קטגוריה 1 התמקדה בקובצי HTML עם טקסט ASCII:

• 1א) HTML אחד לא מקוטע
• 1ב) HTML אחד מקוטע עם JPEG ביניהם
• 1ג) HTML אחד מקוטע עם טקסט Unicode ביניהם
• 1ד) שני קבצי HTML המשולבים זה בזה

PhotoRec אינו משחזר HTML מקוטע בצורה נכונה.

קטגוריה 2 התמקדה במסמכי Microsoft Office:

• 2א) קובץ Word אחד, לא מקוטע
• 2ב) קובץ Word אחד, מקוטע עם 3 שברים ונתונים אקראיים ביניהם
• 2ג) קובץ אקסל אחד מפוצל עם נתונים אקראיים ביניהם
• 2ד) קובץ Word אחד מקוטע עם JPEG בין
• 2ה) קובץ Word אחד מקוטע עם טקסט ביניהם

קטגוריה 3 התמקדה בקובצי JPEG:

• 3א) JPEG אחד לא מקוטע
• 3ב) JPEG אחד לא מקוטע, גדול יותר מגודל קובץ ברירת מחדל אופייני

Machine Translated by Google

- 3ג) JPEGאחד לא מקוטע, אבל למגזר לפניו יש 0xffd8בשני הבתים הראשונים □
- 3d) JPEG אחד מקוטע עם טקסט ביניהם □
- 3ה) JPEGאחד מקוטע עם מסמך Wordבין □
- 3ו) JPEGאחד מפוצל עם נתונים אקראיים ביניהם □
- 3g) JPEG אחד מקוטע עם JPEGביניהם □
- 3h) שני JPEGשלובים זה בזה
- 3i) JPEG אחד לא מקוטע שהוא ממש גדול □
- 3j) JPEG אחד מפוצל עם סקטור אחד ביניהם שמתחיל □ ב-0xffd9

PhotoRec-ליש תוצאות טובות בקטגוריית JPEG.

קטגוריה 4התמקדה בקובצי ZIP:

- 4א) קובץ ZIPאחד, לא מקוטע □
- 4ב) קובץ ZIPאחד מקוטע עם טקסט ביניהם □
- 4ג) קובץ ZIPאחד מפוצל עם נתונים אקראיים ביניהם

2b b0036998.doc 3f f0040638.jpg 3g f0041611.jpg 3g f0043434.05e f0043847 5429-4435 1557-7969 [illegible]	שם הקובץ [illegible]_9000000ff0000000 4608 md5
f0029529_The_Tempest_Entire 3_h_Play b0031533.jpg 2a f0032837_Fact_Sheet_-_Permitted_and_[. . .].doc 2e b0034288.doc 2e f0034399.txt 3c f0036292.jpg	0-8394
1c f0028244_Chapter_cxxxiv_-_THE_CHASE_[. . .].html 28244-28306 (X) 1c f0028307.html 4a f0028439_4n6rodeo3-fix_copy.zip 4b f0028729_file1.zip 4b	18147
2d f0008285.jpg 3d f0011619.jpg 3d f0011823.txt 3b f0012222.jpg 1b f0027496_Comedy_of_Errors.html 1b7jpg f0018234 f0027978.html	4428800 X
f0003868.jpg 1d f0004436_A_STUDY_IN_SCARLET_1.1.html 1d f0004456_1_Stave_1_Marley_s_Ghost.html 1d f00042d .html f0007964_National_Park_Service.doc 3868-4428	287186 □
27607-27977 27978-28196	10240 X 2c b0002051.doc 3a
16128 27496-27606	שבר23544 X 27875
11849-12017 11823-112168	
8285-9473 11619-11822	450048 □
7964-8284 9474-10031	608703 □
4456-4501 4502-4556	190720 □
4436-4455	12828 (+2) X
	7113968 □
	56832 X
	189534 □
	קטע 111693
	31850 X
	18995 קטע28307-28344
	28439-28726 147150 □
	28729-29528 29896-31368 1163745 □
	29529-29895 187793 (-2) X
	31475-31532 29696 X
	31533-31887 181760 X
	32837-33397 287232 □
	34288-34398 34413-36291 36641-36997 1201664 X
	[illegible] קטע
	34399-34412 6781 36292-36640 178659 □
	3133440 X
	487473 □
	1021085 □
	304413 □
	573499 □

ממשיך בעמוד הבא

Machine Translated by Google

טבלה - 1המשך מהעמוד הקודם

924877	94846-95628 95630-96653	3i f0046910.jpg 3j f0094846.jpg
71680 24538540	45964-46103 46910-94836	3e f0045964_Statements_of_Financial_Condition.doc

18.4זיהוי פלילי: כתיבת חוסמים

ניתן לשנות את התוכן של דיסק על ידי חיבורו למחשב:

• מנהל התקן LVMיסנכרן שני אמצעי אחסון דמויי RAID1אם הם לא מסונכרנים
• Linux Raid ו-Fake Raid גם יסנכרנו מחדש את הדיסקים אם הם לא מסונכרנים
• הרכבה אוטומטית של מערכת הקבצים תשנה את תאריך ההרכבה האחרון ואת ספירת ההרכבה
• ext3 ו-ext4 ישחקו את היומן אם מערכת הקבצים מלוכלכת.
• מערכת הקבצים NTFSעשויה לנסות לבצע או להחזיר עסקאות שלא הסתיימו, ו/או לשנות דגלים ב- עוצמת הקול כדי לסמן אותו כ"בשימוש".
• מערכת ההפעלה תעדכן את זמן הגישה לכל קובץ שניגשת אליו
• Windows עשוי ליצור תיקיות נסתרות עבור סל המיחזור או תצורת החומרה השמורה
• זיהומים וירוסים או תוכנות זדוניות במערכת המשמשת לניתוח עלולים לנסות להדביק את הדיסק הנבדק.
• הוספה אוטומטית לאינדקס של הקבצים עשויה ליצור קבצים חדשים בדיסק

בקרי דיסקים משפטיים או חוסמי כתיבה בחומרה קשורים לרוב לתהליך של יצירת תמונת דיסק, או רכישה, במהלך ניתוח משפטי. השימוש בהם הוא כדי למנוע שינוי לא מכוון של ראיות. הגנה על כונן ראיות מפני כתיבה במהלך החקירה חשובה גם כדי להתמודד עם האשמות פוטנציאליות לפיהן תוכן הכונן השתנה במהלך החקירה. כמובן שניתן לטעון זאת בכל מקרה, אך בהיעדר טכנולוגיה להגנה על כונן מפני כתיבה, אין דרך להפריך טענה כזו.

חוסם כתיבה בחומרה מונע שינויים מהמחשב אך אינו מונע מהדיסק לשנות את עצמו (כלומר עדכוני סטטוס SMARTבאזור השירות בכל פעם שהמכשיר מופעל.). זה נשאר הפתרון הטוב ביותר למניעת שינויים מקריים.

ללא חוסם כתיבה בחומרה, עדיין ניתן להפחית את הסיכונים של שינויים מקריים. שימוש במחשב לינוקס ללא ממשק גרפי וללא הרכבה אוטומטית עשוי להיחשב כפתרון מספיק טוב.

תחת לינוקס, ניתן להשתמש blockdev-באו hdparmכדי להעביר דיסק לקריאה בלבד:

```
dev/sdb hdparm -r1 /dev/sdb
blockdev --setro /
```

בפועל, זה לא עובד! TestDiskיפתח את המכשירים האלה בקריאה-כתיבה.

מכשיר Loopbackהוא חלופה בטוחה יותר:

```
dev/loop0 /dev/sdb testdisk /dev/loop0
losetup -r /
```

בדרך זו TestDiskנאלץ לפתוח את המכשיר לקריאה בלבד.

ניתן להשתמש Loopback-בגם לטעינת מערכת קבצים בקריאה בלבד:

Machine Translated by Google


```
p1 mount -o ro /dev/loop0p1 /mnt/p1
sdb partprobe /dev/loop0 mkdir /mnt/
losetup -r /dev/loop0 /dev/
```

בעבודה עם תמונת דיסק (קובץ dmg או raw/dd) תחת mac, גישה לקריאה בלבד אפשרית

```
hdiutil attach -nomount -noverify - תמונה לקריאה בלבד.dd
```

אפשר גם גישת כתיבה ללא שינוי בקובץ המקורי, השינויים יאוחסנו בקובץ צל

```
hdiutil attach -nomount -shadow /path/to/image_shadow_file /path/to/image_file
```

Machine Translated by Google

פֶּרֶק

תֵשַׁע עֶשׂרֵה

LINUX / MACOS / BSD COMMAND LINE

שורת הפקודה היא ממשק טקסט למחשב / NASשלך. זה מכונה לעתים קרובות מעטפת, מסוף, קונסולה, הנחיה. מדריך קצר זה ייתן לך כמה פקודות ומושגים בסיסיים.

19.1הפעלת מסוף

כדי לפתוח טרמינל

• אם המחשב שלך באמת מריץ לינוקס עם ממשקים גרפיים של :Gnome

- בחר "פעילויות" בצד שמאל למעלה
- בהנחיה "הקלד לחיפוש", הקלד מסוף
- לחץ על סמל "טרמינל".

• אם במחשב שלך פועל macox

– הקש Command+Space והקלד Terminal ולחץ על מקש .Enter/Return
- הפעל באפליקציית טרמינל

• אם במחשב שלך פועל Windows וברצונך להתחבר ל-SAN שלך באמצעות ssh

- השתמש בלקוח ssh כמו Putty

• אם במחשב שלך פועל Linux או macos ואתה רוצה להתחבר ל-SAN שלך באמצעות ssh

– הקש Command+Space והקלד Terminal ולחץ על מקש .Enter/Return
- הפעל באפליקציית טרמינל
– ssh root@192.168.0.1 (החלף את השורש במידת הצורך ואת 192.168.0.1 ב-PI הנכון)

19.2משתמשים

משתמש השורש הוא משתמש הרשאות ברירת המחדל. בדרך כלל, ההנחיה הטרמינל מסתיימת ב-'#' עבור root וב-'$' עבור המשתמשים האחרים. כדי לבדוק את המשתמש הנוכחי, השתמש ב-di. כדי להפוך לשורש מחשבון משתמש, אתה יכול לנסות

• sudo -s ייתכן שתתבקש להזין את סיסמת המשתמש שלך.

• su - ייתכן שיהיה עליך להקליד את סיסמת השורש.

לא יהיה הד בעת הקלדת הסיסמה.

Machine Translated by Google

19.3מערכת קבצים

• שמות קבצים, נתיבים ופקודות הם תלויי רישיות. אתה צריך לכבד את ABC-ההעליון וה-cba התחתון מקרים.

• כל הקבצים הנגישים במערכת Unixמסודרים בעץ אחד גדול, היררכיית הקבצים, המושרשים ב- /. •למשתמש השורש יש גישה לכל קבצים, ספריות ופקודות[1]

• פקודת mount-המשמשת לצרף את מערכת הקבצים שנמצאת במכשיר כלשהו לעץ הקבצים הגדול.

• לעומת זאת, הפקודה umountתנתק אותו שוב.

• בעת שימוש בממשק גרפי, ניתן לבצע פעולות mount ו-umountעל ידי כמה לחיצות עכבר על הסמלים המייצג את המכשיר.

• בעת שימוש בשורת הפקודה, נדרשות הרשאות שורש.

• נקודת ההרכבה היא שם הספרייה שבה מחובר המכשיר. לפי המוסכמה, זה בדרך כלל ב- / mnt, /media ואו /run/media.

19.4פקודות

• cd directory_name: שנה את הספרייה הנוכחית

• pwd: הדפס ספריית עבודה

• ls: רשימת קבצים מהספרייה הנוכחית (קבצים שמתחילים בנקודה אינם רשומים כברירת מחדל)

• ./testdisk_static: הפעל את התוכנית testdisk_staticבהנחה שהיא קיימת בספרייה הנוכחית.

• testdisk: הפעל testdiskאם הפקודה נמצאת ברשימה של ספריות-PATH, זה לא ינסה להפעיל שם מתוכנת testdiskבספרייה הנכונה.

[1] · גישת שורש עשויה להיות מוגבלת על ידי בקרת גישה מבוססת תפקידים (RBAC)אבטחה מרובת רמות . .(MLS).