Tworzenie kopii nośnika za pomocą dc3dd razem z porównaniem hashy
Kopiowanie:

```
┌──(kali㉿kali)-[~/sledcza]
└─$ sudo dc3dd if=/dev/sdb hof=sandisk hash=md5

dc3dd 7.2.646 started at 2023-01-23 06:50:03 -0500
compiled options:
command line: dc3dd if=/dev/sdb hof=sandisk hash=md5
device size: 60088320 sectors (probed),   30,765,219,840 bytes
sector size: 512 bytes (probed)
 5944213504 bytes ( 5.5 G ) copied ( 19% ),  184 s, 31 M/s
```

Hashowanie:

```
┌──(kali㉿kali)-[~/sledcza]
└─$ sudo dc3dd if=/dev/sdb hof=sandisk hash=md5

dc3dd 7.2.646 started at 2023-01-23 06:50:03 -0500
compiled options:
command line: dc3dd if=/dev/sdb hof=sandisk hash=md5
device size: 60088320 sectors (probed),   30,765,219,840 bytes
sector size: 512 bytes (probed)
 2686484480 bytes ( 2.5 G ) hashed (  9% ),    7 s, 375 M/s
```

Hashe się zgadzają:

```
┌──(kali㉿kali)-[~/sledcza]
└─$ sudo dc3dd if=/dev/sdb hof=sandisk hash=md5

dc3dd 7.2.646 started at 2023-01-23 06:50:03 -0500
compiled options:
command line: dc3dd if=/dev/sdb hof=sandisk hash=md5
device size: 60088320 sectors (probed),   30,765,219,840 bytes
sector size: 512 bytes (probed)
 30765219840 bytes ( 29 G ) copied ( 100% ), 1006 s, 29 M/s
 30765219840 bytes ( 29 G ) hashed ( 100% ),   77 s, 383 M/s

input results for device `/dev/sdb':
   60088320 sectors in
   0 bad sectors replaced by zeros
   25e731daf4597d2b30e2141112283a38 (md5)

output results for file `sandisk':
   60088320 sectors out
   [ok] 25e731daf4597d2b30e2141112283a38 (md5)

dc3dd completed at 2023-01-23 07:06:49 -0500
```

Informacje o partycjach

```
┌──(kali㉿kali)-[~/sledcza]
└─$ mmls sandisk
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  ------    0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0060088319   0060086272   NTFS / exFAT (0x07)
```

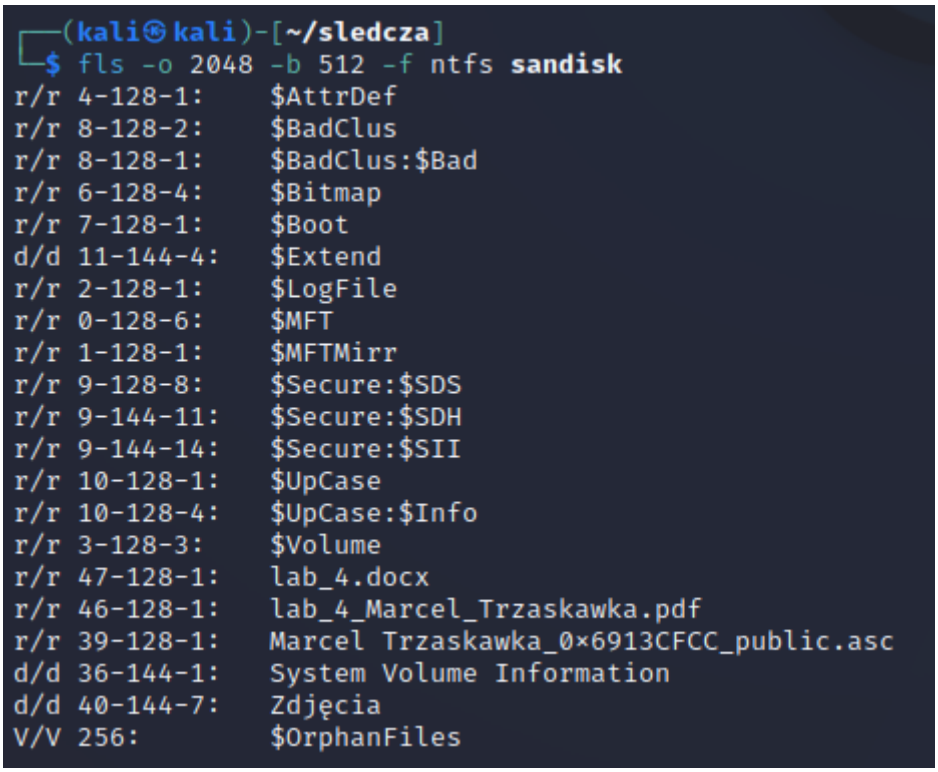
Partycja główna tego pendrive’a jest w formacie NTFS
Offset wynosi 2048 512-bajtowych sektorów

Aby wyświetlić informacje na temat tego systemu plików trzeba podać offset

```
┌──(kali㉿kali)-[~/sledcza]
└─$ fsstat -o 2048 -f ntfs sandisk
FILE SYSTEM INFORMATION
--------------------------------------------

File System Type: NTFS
Volume Serial Number: 5ACAD1A0CAD17929
OEM Name: NTFS
Volume Name: Sandisk
Version: Windows XP

METADATA INFORMATION
--------------------------------------------

First Cluster of MFT: 786432
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 256
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------

Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 7510782
Total Sector Range: 0 - 60086270

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit   Flags: Non-resident
$VOLUME_NAME (96)   Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)   Size: No Limit   Flags:
$INDEX_ROOT (144)   Size: No Limit   Flags: Resident
$INDEX_ALLOCATION (160)   Size: No Limit   Flags: Non-resident
$BITMAP (176)   Size: No Limit   Flags: Non-resident
$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident
```

Typ systemu plików: NTFS
Numer seryjny partycji: 5ACAD1A0CAD17929
Nazwa partycji: Sandisk
Sector size: 512
Cluster size: 4096

FLS



-o – offset w sektorach
-b – rozmiar sektora
-f – typ systemu plików

Zauważyć można tutaj plik docx, plik pdf, plik prawdopodobnie z kluczem publicznym RSA oraz katalog ze zdjęciami
Nie ma usuniętych plików

Aby zobaczyć co znajduje się w katalogach wystarczy dodać opcję -r (Recursive)

```
┌──(kali㉿kali)-[~/sledcza]
└─$ fls -o 2048 -b 512 -f ntfs -r sandisk
r/r 4-128-1:    $AttrDef
r/r 8-128-2:    $BadClus
r/r 8-128-1:    $BadClus:$Bad
r/r 6-128-4:    $Bitmap
r/r 7-128-1:    $Boot
d/d 11-144-4:   $Extend
+ d/d 29-144-2: $Deleted
+ r/r 25-144-2: $ObjId:$O
+ r/r 24-144-3: $Quota:$O
+ r/r 24-144-2: $Quota:$Q
+ r/r 26-144-2: $Reparse:$R
+ d/d 27-144-2: $RmMetadata
++ r/r 28-128-4:        $Repair
++ r/r 28-128-2:        $Repair:$Config
++ d/d 31-144-2:        $Txf
++ d/d 30-144-2:        $TxfLog
+++ r/r 32-128-2:       $Tops
+++ r/r 32-128-4:       $Tops:$T
+++ r/r 33-128-1:       $TxfLog.blf
+++ r/r 34-128-1:       $TxfLogContainer00000000000000000001
+++ r/r 35-128-1:       $TxfLogContainer00000000000000000002
r/r 2-128-1:    $LogFile
r/r 0-128-6:    $MFT
r/r 1-128-1:    $MFTMirr
r/r 9-128-8:    $Secure:$SDS
r/r 9-144-11:   $Secure:$SDH
r/r 9-144-14:   $Secure:$SII
r/r 10-128-1:   $UpCase
r/r 10-128-4:   $UpCase:$Info
r/r 3-128-3:    $Volume
r/r 47-128-1:   lab_4.docx
r/r 46-128-1:   lab_4_Marcel_Trzaskawka.pdf
r/r 39-128-1:   Marcel Trzaskawka_0×6913CFCC_public.asc
d/d 36-144-1:   System Volume Information
+ r/r 38-128-1: IndexerVolumeGuid
+ r/r 37-128-1: WPSettings.dat
d/d 40-144-7:   Zdjęcia
+ r/r 42-128-1: Kraków.jpg
+ r/r 42-128-3: Kraków.jpg:Zone.Identifier
+ r/r 43-128-1: msagh.jpg
+ r/r 43-128-3: msagh.jpg:Zone.Identifier
+ r/r 45-128-1: szklarska.jpg
+ r/r 45-128-3: szklarska.jpg:Zone.Identifier
+ r/r 44-128-1: tiktok.mp4
+ r/r 44-128-4: tiktok.mp4:Zone.Identifier
+ r/r 41-128-1: widok_chojnik.jpg
+ r/r 41-128-3: widok_chojnik.jpg:Zone.Identifier
V/V 256:        $OrphanFiles
```

W katalogu ze zdjęciami faktycznie znajdują się zdjęcia, oraz plik mp4

MOUNT

Aby móc zobaczyć fizycznie pliki należy ten obraz zamontować
Najpierw należy utworzyć urządzenie loop

```
┌──(kali㉿kali)-[~/sledcza]
└─$ sudo losetup -r -o $((512 * 2048)) /dev/loop0 ~/sledcza/sandisk
[sudo] password for kali:
```

-r – Read-only
-o – Offset (w bajtach!)

```
┌──(kali㉿kali)-[~/sledcza]
└─$ losetup -a
/dev/loop0: []: (/home/kali/sledcza/sandisk), offset 1048576
```

Urządzenie utworzone pomyślnie

Weryfikacja

```
┌──(kali㉿kali)-[~/sledcza]
└─$ sudo fls /dev/loop0
r/r 4-128-1:    $AttrDef
r/r 8-128-2:    $BadClus
r/r 8-128-1:    $BadClus:$Bad
r/r 6-128-4:    $Bitmap
r/r 7-128-1:    $Boot
d/d 11-144-4:   $Extend
r/r 2-128-1:    $LogFile
r/r 0-128-6:    $MFT
r/r 1-128-1:    $MFTMirr
r/r 9-128-8:    $Secure:$SDS
r/r 9-144-11:   $Secure:$SDH
r/r 9-144-14:   $Secure:$SII
r/r 10-128-1:   $UpCase
r/r 10-128-4:   $UpCase:$Info
r/r 3-128-3:    $Volume
r/r 47-128-1:   lab_4.docx
r/r 46-128-1:   lab_4_Marcel_Trzaskawka.pdf
r/r 39-128-1:   Marcel Trzaskawka_0×6913CFCC_public.asc
d/d 36-144-1:   System Volume Information
d/d 40-144-7:   Zdjęcia
V/V 256:        $OrphanFiles
```

Montowanie

```
┌──(kali㉿kali)-[/mnt]
└─$ sudo mount -r /dev/loop0 sandisk

┌──(kali㉿kali)-[/mnt]
└─$ ls
sandisk
```

Widać tu wszystkie pliki

```
┌──(kali㉿kali)-[/mnt/sandisk]
└─$ ls
 lab_4.docx                    'Marcel Trzaskawka_0×6913CFCC_public.asc'   Zdjęcia
 lab_4_Marcel_Trzaskawka.pdf   'System Volume Information'
```

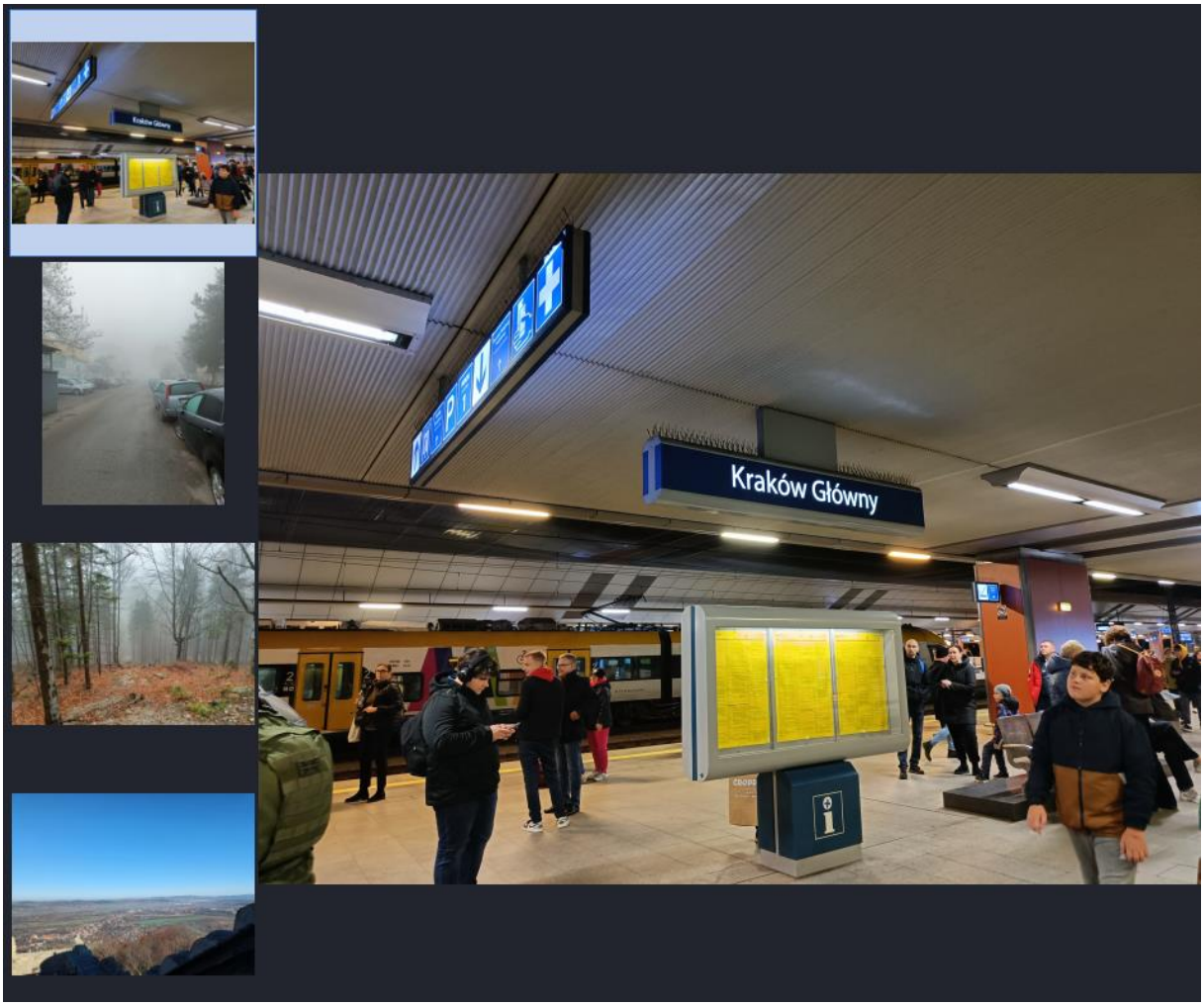
Przykładowe informacje z pliku pdf

```
┌──(kali㉿kali)-[/mnt/sandisk]
└─$ pdfinfo lab_4_Marcel_Trzaskawka.pdf
Author:          Marcel Trzaskawka
Creator:         Microsoft® Word dla Microsoft 365
Producer:        Microsoft® Word dla Microsoft 365
CreationDate:    Wed Dec 28 15:05:44 2022 EST
ModDate:         Wed Dec 28 15:05:44 2022 EST
Custom Metadata: no
Metadata Stream: yes
Tagged:          yes
UserProperties:  no
Suspects:        no
Form:            none
JavaScript:      no
Pages:           9
Encrypted:       no
Page size:       595.32 x 841.92 pts (A4)
Page rot:        0
File size:       1411452 bytes
Optimized:       no
PDF version:     1.7
```

Potwierdzam również, że jest to klucz publiczny

```
┌──(kali㉿kali)-[/mnt/sandisk]
└─$ cat Marcel\ Trzaskawka_0×6913CFCC_public.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEY85o4RYJKwYBBAHaRw8BAQdAKnzQnHGYqTLp1N9EgJPc2IIclyEDOSoYzIpj
FDsJWVG0EU1hcmNlbCBUcnphc2thd2thiJkEExYKAEEWIQSswRYLnnWKTQNfWDY8
wQt7aRPPzAUCY85o4QIbAwUJA8O4TwULCQgHAgIiAgYVCgkICwIEFgIDAQIeBwIX
gAAKCRA8wQt7aRPPzA++AP9/Sk6t0yiKf6f7qjfDMx8zZKCxg7DnU53B1PapW6Us
XAEA3TiOT9yGaTlBa16C6ZfWkJ2OFrSp/DmmZiPaR7+/swa4OARjzmjhEgorBgEE
AZdVAQUBAQdAodESqWFaobw1WDt70SOmx/MoSRBF5C3Snj6UBAqnqBMDAQgHiH4E
GBYKACYWIQSswRYLnnWKTQNfWDY8wQt7aRPPzAUCY85o4QIbDAUJA8O4TwAKCRA8
wQt7aRPPzAOCAP0RPzhOcEFxHtzWnXMqpE1RTp3KnYiDxpVuYIvy9dWITAEApE2/
oQTYe9LdBxxFtFRlULv/Qv1SL4nmaDhxTOl59gs=
=9im4
-----END PGP PUBLIC KEY BLOCK-----
```

Są też tu widoczne zdjęcia



A na nagraniu jest słodki króliczek

Analiza zdjęć w ramach odzyskiwania usuniętych zdjęć

EWF-TOOLS

Pozyskanie obrazu dysku za pomocą ewfacquire

```
┌──(kali㉿kali)-[~/sledcza]
└─$ sudo ewfacquire -t sandisk /dev/sdb
ewfacquire 20140813
```

```
The following acquiry parameters were provided:
Image path and filename:                sandisk.E01
Case number:                            1
Description:
Evidence number:                        1
Examiner name:                          Marcel
Notes:
Media type:                             removable disk
Is physical:                            yes
EWF file format:                        EnCase 6 (.E01)
Compression method:                     deflate
Compression level:                      none
Acquiry start offset:                   0
Number of bytes to acquire:             28 GiB (30765219840 bytes)
Evidence segment file size:             1.4 GiB (1572864000 bytes)
Bytes per sector:                       512
Block size:                             64 sectors
Error granularity:                      64 sectors
Retries on read error:                  2
Zero sectors on read error:             no
```

```
Written: 28 GiB (30765220028 bytes) in 5 minute(s) and 34 second(s) with 87 MiB/s (92111437 bytes/second).
MD5 hash calculated over data:          39f3d49bc277e0332cdc73c2235d5fa8
ewfacquire: SUCCESS
```

```
┌──(kali㉿kali)-[~/sledcza]
└─$ sudo md5sum /dev/sdb
[sudo] password for kali:
39f3d49bc277e0332cdc73c2235d5fa8  /dev/sdb
```

Hashe się zgadzają

Informacje o obrazie

```
┌──(kali㉿kali)-[~/sledcza]
└─$ ewfinfo sandisk.E*
ewfinfo 20140813

Acquiry information
        Case number:            1
        Examiner name:          Marcel
        Evidence number:        1
        Acquisition date:       Mon Jan 23 08:30:16 2023
        System date:            Mon Jan 23 08:30:16 2023
        Operating system used:  Linux
        Software version used:  20140813
        Password:               N/A
        Model:                  SanDisk 3.2Gen
        Serial number:          05013a1728702951763c

EWF information
        File format:            EnCase 6
        Sectors per chunk:      64
        Error granularity:      64
        Compression method:     deflate
        Compression level:      no compression

Media information
        Media type:             removable disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      60088320
        Media size:             28 GiB (30765219840 bytes)

Digest hash information
        MD5:                    39f3d49bc277e0332cdc73c2235d5fa8
```

Montowanie za pomocą ewfmount

```
┌──(kali㉿kali)-[/mnt]
└─$ sudo mkdir ewf

┌──(kali㉿kali)-[/mnt]
└─$ sudo chown kali ewf

┌──(kali㉿kali)-[/mnt]
└─$ ewfmount ~/sledcza/sandisk.E01 ewf
ewfmount 20140813
```

```
┌──(kali㉿kali)-[/mnt]
└─$ cd ewf

┌──(kali㉿kali)-[/mnt/ewf]
└─$ ls
ewf1
```

Ewf1 to surowy obraz dysku, na którym możemy teraz zastosować narzędzia nie znające formatu ewf

```
┌──(kali㉿kali)-[/mnt/ewf]
└─$ mmls ewf1
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
000: Meta    0000000000   0000000000   0000000001   Primary Table (#0)
001: ------  0000000000   0000002047   0000002048   Unallocated
002: 000:000 0000002048   0060088319   0060086272   NTFS / exFAT (0x07)
```

```
┌──(kali㉿kali)-[/mnt/ewf]
└─$ fsstat -o 2048 -f ntfs ewf1
FILE SYSTEM INFORMATION
--------------------------------------------

File System Type: NTFS
Volume Serial Number: 5ACAD1A0CAD17929
OEM Name: NTFS
Volume Name: Sandisk
Version: Windows XP

METADATA INFORMATION
--------------------------------------------

First Cluster of MFT: 786432
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 256
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------

Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 7510782
Total Sector Range: 0 - 60086270

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit   Flags: Non-resident
$VOLUME_NAME (96)   Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)   Size: No Limit   Flags:
$INDEX_ROOT (144)   Size: No Limit   Flags: Resident
$INDEX_ALLOCATION (160)   Size: No Limit   Flags: Non-resident
$BITMAP (176)   Size: No Limit   Flags: Non-resident
$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident
```