Przygotowanie do odzyskiwania zdjęć

```
┌──(kali㉿kali)-[~/sledcza]
└─$ sudo dc3dd wipe=/dev/sdb

dc3dd 7.2.646 started at 2023-01-23 10:42:26 -0500
compiled options:
command line: dc3dd wipe=/dev/sdb
device size: 60088320 sectors (probed),   30,765,219,840 bytes
sector size: 512 bytes (probed)
 1084817408 bytes ( 1 G ) copied (  4% ),    3 s, 381 M/s
```

Wyczyszczenie całego pendrive'a

```
┌──(kali㉿kali)-[~/sledcza]
└─$ sudo dc3dd wipe=/dev/sdb

dc3dd 7.2.646 started at 2023-01-23 10:42:26 -0500
compiled options:
command line: dc3dd wipe=/dev/sdb
device size: 60088320 sectors (probed),   30,765,219,840 bytes
sector size: 512 bytes (probed)
 30765219840 bytes ( 29 G ) copied ( 100% ), 1380 s, 21 M/s

input results for pattern `00':
   60088320 sectors in

output results for device `/dev/sdb':
   60088320 sectors out

dc3dd completed at 2023-01-23 11:05:26 -0500
```

Skopiowanie plików na usb, a następnie ich usunięcie

```
┌──(kali㉿kali)-[/media/kali/6BEE-FED4]
└─$ ls
 lab_4.docx   lab_4_Marcel_Trzaskawka.pdf  'Marcel Trzaskawka_0×6913CFCC_public.asc'   Zdjęcia

┌──(kali㉿kali)-[/media/kali/6BEE-FED4]
└─$ rm -rf ./*
zsh: sure you want to delete all 4 files in /media/kali/6BEE-FED4/. [yn]? y
```

Stworzenie 300 MB pliku na USB

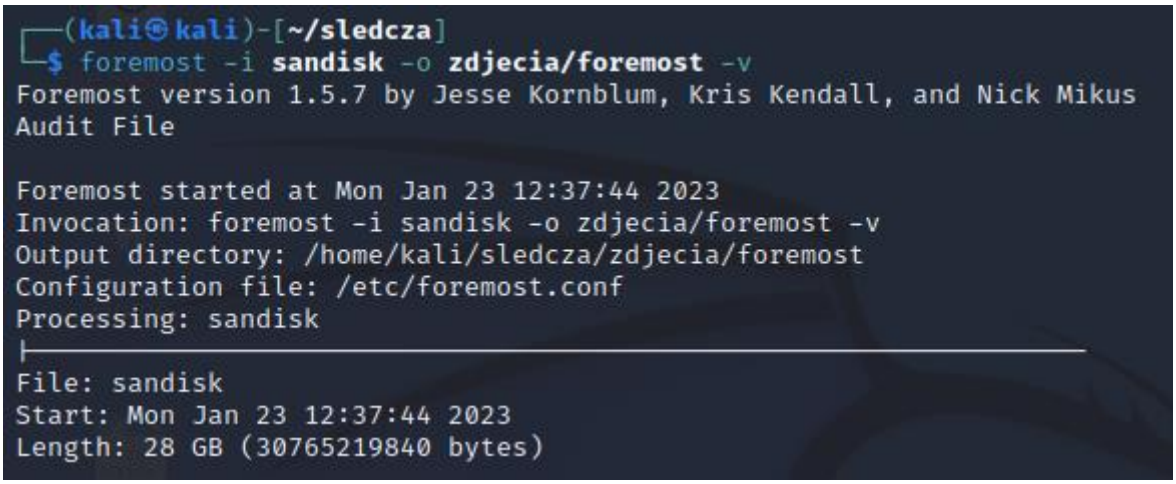
```
┌──(kali㉿kali)-[~/sledcza]
└─$ dd if=/dev/random of=/media/kali/6BEE-FED4/random
^C596313+0 records in
596313+0 records out
305312256 bytes (305 MB, 291 MiB) copied, 1.84692 s, 165 MB/s
```

Utworzenie obrazu dysku

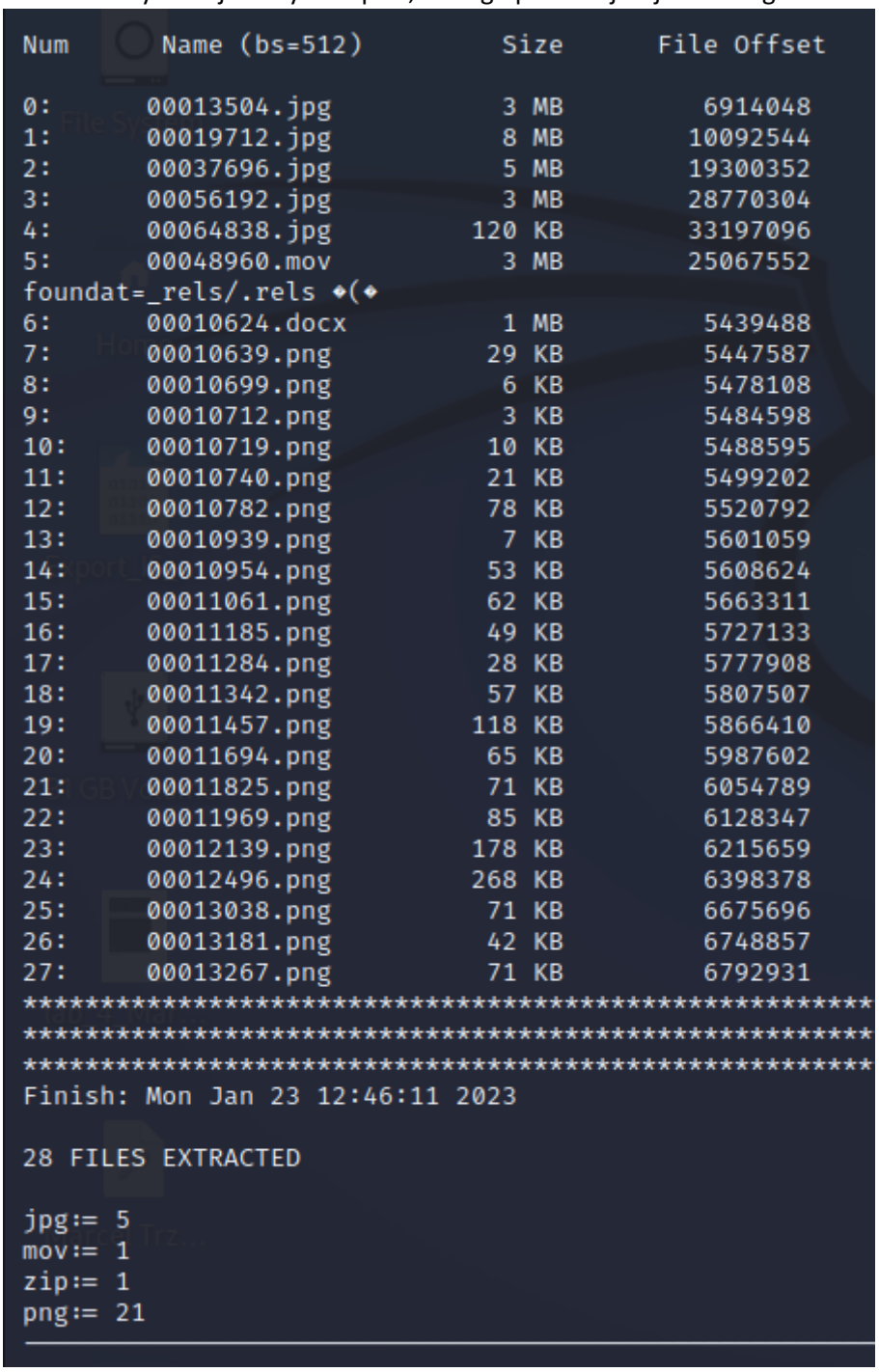
```
┌──(kali㉿kali)-[~/sledcza]
└─$ sudo dc3dd if=/dev/sdb hof=sandisk hash=md5

dc3dd 7.2.646 started at 2023-01-23 12:13:14 -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)
  118226944 bytes ( 113 M ) copied (  0% ),    4 s, 31 M/s
```

# FOREMOST

Aby ozdyskać dane z obrazu za pomocą foremost wystarczy proste polecenie



Foremost wyszukuje wszystkie pliki, dlatego praca zajmuje mu długo



```
Num     Name (bs=512)         Size      File Offset

0:      00013504.jpg           3 MB         6914048
1:      00019712.jpg           8 MB        10092544
2:      00037696.jpg           5 MB        19300352
3:      00056192.jpg           3 MB        28770304
4:      00064838.jpg         120 KB        33197096
5:      00048960.mov           3 MB        25067552
foundat=_rels/.rels ♦(♦
6:      00010624.docx          1 MB         5439488
7:      00010639.png          29 KB         5447587
8:      00010699.png           6 KB         5478108
9:      00010712.png           3 KB         5484598
10:     00010719.png          10 KB         5488595
11:     00010740.png          21 KB         5499202
12:     00010782.png          78 KB         5520792
13:     00010939.png           7 KB         5601059
14:     00010954.png          53 KB         5608624
15:     00011061.png          62 KB         5663311
16:     00011185.png          49 KB         5727133
17:     00011284.png          28 KB         5777908
18:     00011342.png          57 KB         5807507
19:     00011457.png         118 KB         5866410
20:     00011694.png          65 KB         5987602
21:     00011825.png          71 KB         6054789
22:     00011969.png          85 KB         6128347
23:     00012139.png         178 KB         6215659
24:     00012496.png         268 KB         6398378
25:     00013038.png          71 KB         6675696
26:     00013181.png          42 KB         6748857
27:     00013267.png          71 KB         6792931
*************************************************************
*************************************************************
*************************************************************
Finish: Mon Jan 23 12:46:11 2023

28 FILES EXTRACTED

jpg:= 5
mov:= 1
zip:= 1
png:= 21
-------------------------------------------------------------
```

Foremost odzyskał wszystkie pliki, a nawet wyodrębnił pliki png z pliku docx

# RECOVERJPEG

```
┌──(kali㉿kali)-[~/sledcza]
└─$ recoverjpeg sandisk -v -o zdjecia/recoverjpeg
Candidate jpeg found
   Found section e1 of len 2044
   Found section e2 of len 3160
   Found section e5 of len 65406
   Found section e6 of len 65406
   Found section e7 of len 65406
   Found section e8 of len 65406
   Found section db of len 67
   Found section db of len 67
   Found section c0 of len 17
   Found section c4 of len 31
   Found section c4 of len 181
   Found section c4 of len 31
   Found section c4 of len 181
   Found section da of len 12
   Looking for end marker... found at offset 3162275
   Found end of image after 3162278 bytes
image00000.jpg 3162277 bytes
```

Recoverjpeg zadziałał szybciej niż foremost, ponieważ wyszukiwał tylko obrazów, a nie wszelkich rodzajów plików

Odnalazł jednak tylko 3 pliki

```
┌──(kali㉿kali)-[~/sledcza/zdjecia/recoverjpeg]
└─$ ls
image00000.jpg  image00001.jpg  image00002.jpg
```

# SCALPEL

Odkomentowałem w pliku konfiguracyjnym linie z headerami i footerami plików, które chciałem odzyskać

```
┌──(kali㉿kali)-[~/sledcza]
└─$ scalpel sandisk -o zdjecia/scalpel
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/kali/sledcza/sandisk"

Image file pass 1/2.
sandisk: 100.0% |*****************************************************************************|   28.7 GB    00:00 ETA
Allocating work queues ...
Work queues allocation complete. Building carve lists ...
Carve lists built.  Workload:
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x45\x78\x69\x66" and footer "\xff\xd9" --> 4 files
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x4a\x46\x49\x46" and footer "\xff\xd9" --> 1 files
png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 0 files
png with header "\x89\x50\x4e\x47\x0d\x0a\x1a\x0a" and footer "\x00\x00\x00\x00\x49\x45\x4e\x44" --> 21 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" and footer "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" --
> 0 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1" and footer "" --> 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" --> 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" --> 0 files
zip with header "\x50\x4b\x03\x04" and footer "\x3c\xac" --> 33 files
Carving files from image.
Image file pass 2/2.
sandisk: 100.0% |*****************************************************************************|   28.7 GB    00:00 ETA
Processing of image file complete. Cleaning up ...
Done.
Scalpel is done, files carved = 59, elapsed = 325 seconds.
```

```
┌──(kali㉿kali)-[~/sledcza/zdjecia/scalpel/jpg-0-0]
└─$ ls
00000000.jpg  00000001.jpg  00000002.jpg  00000003.jpg

┌──(kali㉿kali)-[~/sledcza/zdjecia/scalpel/jpg-0-0]
└─$ cd ../jpg-1-0

┌──(kali㉿kali)-[~/sledcza/zdjecia/scalpel/jpg-1-0]
└─$ ls
00000004.jpg

┌──(kali㉿kali)-[~/sledcza/zdjecia/scalpel/jpg-1-0]
└─$ cd ../png-3-0

┌──(kali㉿kali)-[~/sledcza/zdjecia/scalpel/png-3-0]
└─$ ls
00000005.png  00000008.png  00000011.png  00000014.png  00000017.png  00000020.png  00000023.png
00000006.png  00000009.png  00000012.png  00000015.png  00000018.png  00000021.png  00000024.png
00000007.png  00000010.png  00000013.png  00000016.png  00000019.png  00000022.png  00000025.png

┌──(kali㉿kali)-[~/sledcza/zdjecia/scalpel/png-3-0]
└─$ cd ../zip-8-0

┌──(kali㉿kali)-[~/sledcza/zdjecia/scalpel/zip-8-0]
└─$ ls
00000026.zip  00000031.zip  00000036.zip  00000041.zip  00000046.zip  00000051.zip  00000056.zip
00000027.zip  00000032.zip  00000037.zip  00000042.zip  00000047.zip  00000052.zip  00000057.zip
00000028.zip  00000033.zip  00000038.zip  00000043.zip  00000048.zip  00000053.zip  00000058.zip
00000029.zip  00000034.zip  00000039.zip  00000044.zip  00000049.zip  00000054.zip
00000030.zip  00000035.zip  00000040.zip  00000045.zip  00000050.zip  00000055.zip
```

Scalpel odzyskał wszystkie zdjęcia jpg, png z docxa, docx nie został odzyskany, prawdopodobnie jest rozbity na zip

# Analiza zdjęć

Aby szybko przeanalizować zdjęcia używając Exiftool, dopisałem interesujące mnie tagi.

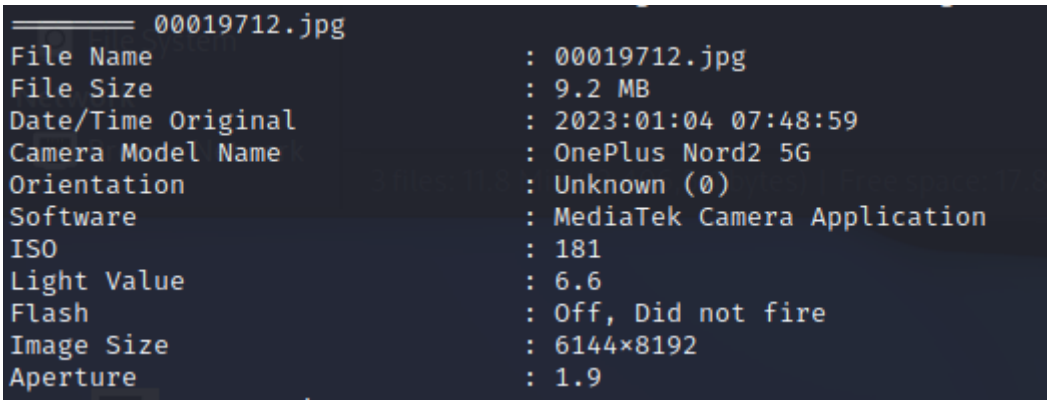
Polecenie wygląda tak:
*exiftool -FileName -FileSize -DateTimeOriginal -Model -Orientation -Software -ISO -LightValue -Flash -ImageSize -Aperture -GPSPosition -LensModel **

```
======== 00013504.jpg
File Name                       : 00013504.jpg
File Size                       : 3.2 MB
Date/Time Original              : 2022:11:07 18:32:50
Camera Model Name               : OnePlus Nord2 5G
Orientation                     : Horizontal (normal)
Software                        : MediaTek Camera Application
ISO                             : 1779
Light Value                     : 3.3
Flash                           : Off, Did not fire
Image Size                      : 4096×3072
Aperture                        : 1.9
GPS Position                    : 50 deg 4' 5.09" N, 19 deg 56' 49.80" E
```

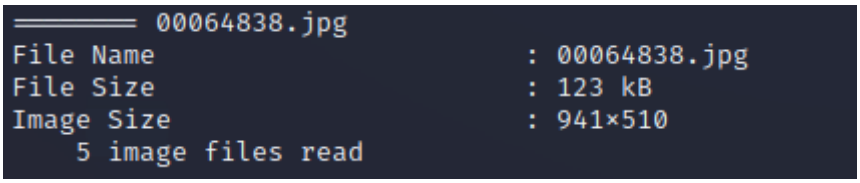
```
======== 00037696.jpg
File Name                       : 00037696.jpg
File Size                       : 5.8 MB
Date/Time Original              : 2022:11:05 08:26:11
Camera Model Name               : OnePlus Nord2 5G
Orientation                     : Horizontal (normal)
Software                        : MediaTek Camera Application
ISO                             : 237
Light Value                     : 6.2
Flash                           : Off, Did not fire
Image Size                      : 4096×3072
Aperture                        : 1.9
```

```
======== 00056192.jpg
File Name                       : 00056192.jpg
File Size                       : 3.5 MB
Date/Time Original              : 2022:11:06 11:31:34
Camera Model Name               : OnePlus Nord2 5G
Orientation                     : Horizontal (normal)
Software                        : MediaTek Camera Application
ISO                             : 105
Light Value                     : 12.1
Flash                           : Off, Did not fire
Image Size                      : 4096×3072
```

Te 3 zdjęcia zostały wykonane w przeciągu 3 dni
Tylko jedno z nich posiada lokalizację
Zostało wykonane na Dworcu Głównym w Krakowie




To zdjęcie zostało wykonane 4.01.2023 i ma 4 krotnie większy rozmiar w pixelach niż pozostałe




Ostatnie zdjęcie ma dostępne mało informacji

Ta analiza została dokonana na zdjęciach odzyskanych za pomocą foremost
Oryginalnie zdjęć było 4 i wszystkie mają takie same wartości jak te odzyskane
Piąte zdjęcie jest to zrzut ekranu który znajdował się w pliku docx