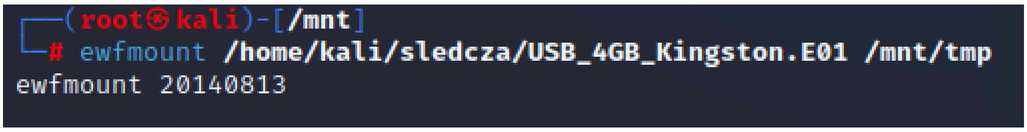
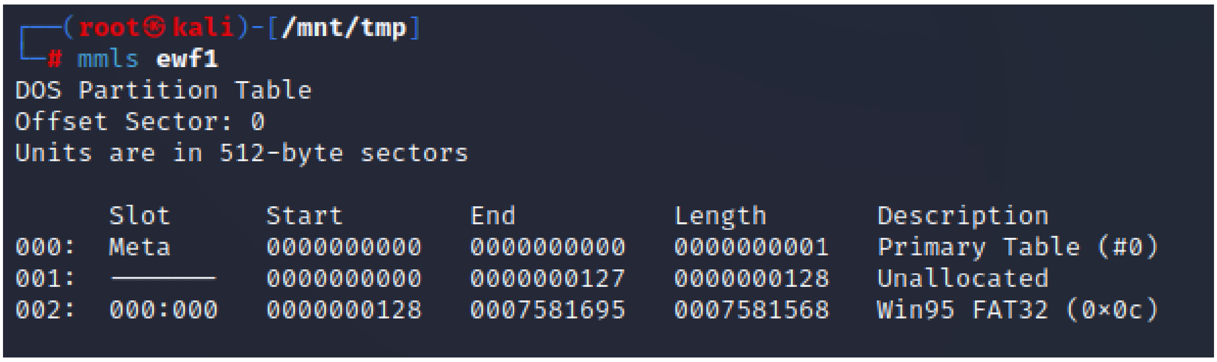
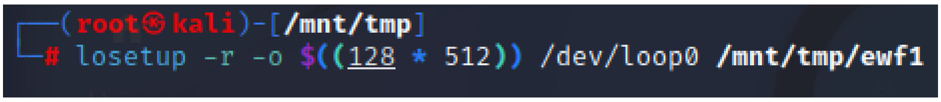


```
┌──(root㉿kali)-[/mnt]
└─# ewfmount /home/kali/sledcza/USB_4GB_Kingston.E01 /mnt/tmp
ewfmount 20140813
```

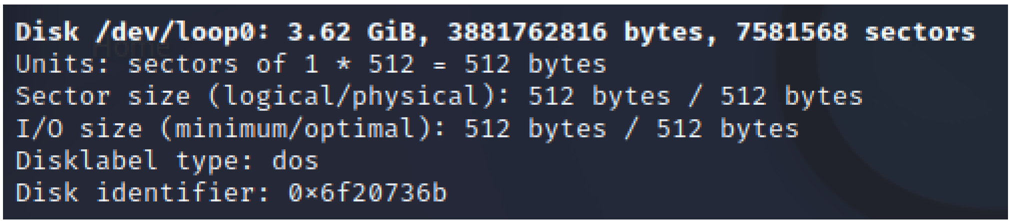


```
┌──(root㉿kali)-[/mnt/tmp]
└─# mmls ewf1
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000000127   0000000128   Unallocated
002:  000:000   0000000128   0007581695   0007581568   Win95 FAT32 (0×0c)
```

Partycja z danymi znajduje się w sektorze 128

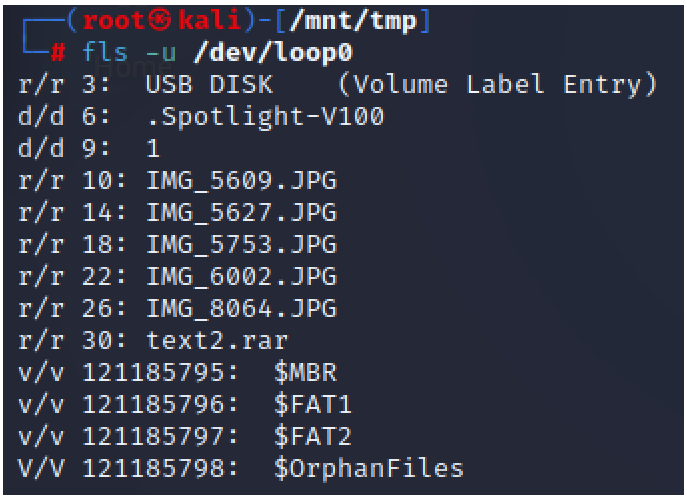


```
┌──(root㉿kali)-[/mnt/tmp]
└─# losetup -r -o $((128 * 512)) /dev/loop0 /mnt/tmp/ewf1
```



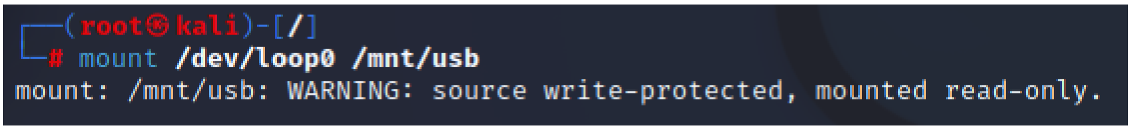
```
Disk /dev/loop0: 3.62 GiB, 3881762816 bytes, 7581568 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0×6f20736b
```

Dla upewnienia się, że udało się zamontować loop poprawnie:

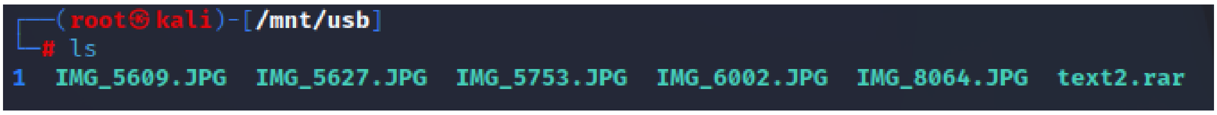


```
┌──(root㉿kali)-[/mnt/tmp]
└─# fls -u /dev/loop0
r/r 3:  USB DISK    (Volume Label Entry)
d/d 6:  .Spotlight-V100
d/d 9:  1
r/r 10: IMG_5609.JPG
r/r 14: IMG_5627.JPG
r/r 18: IMG_5753.JPG
r/r 22: IMG_6002.JPG
r/r 26: IMG_8064.JPG
r/r 30: text2.rar
v/v 121185795:  $MBR
v/v 121185796:  $FAT1
v/v 121185797:  $FAT2
V/V 121185798:  $OrphanFiles
```

Aby mieć dostęp do plików /dev/loop0 należy zamontować:

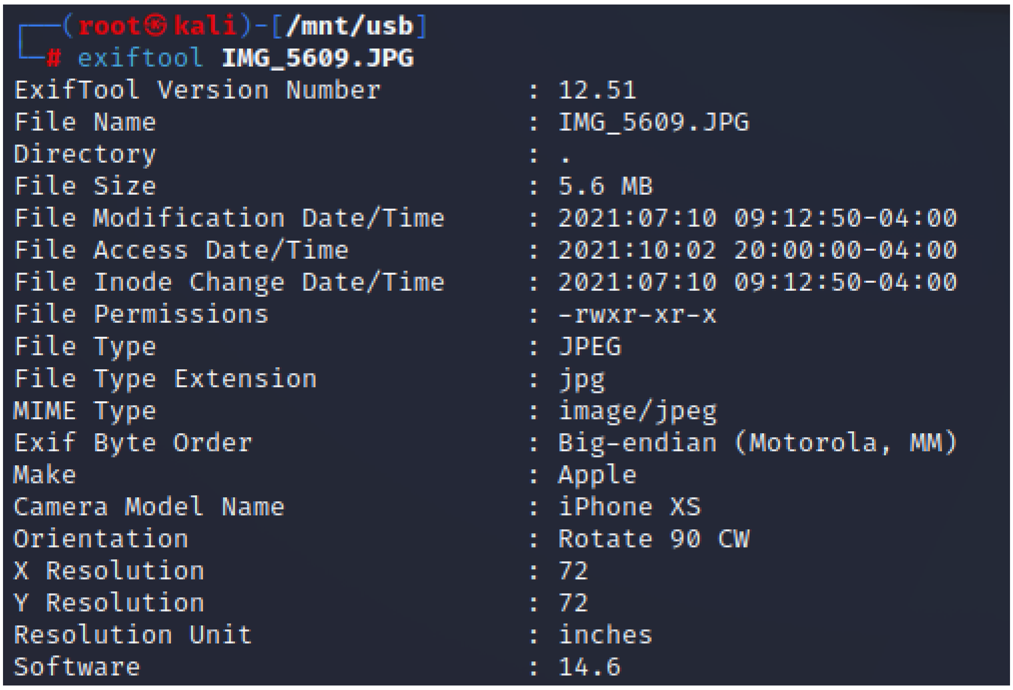


```
┌──(root㉿kali)-[/]
└─# mount /dev/loop0 /mnt/usb
mount: /mnt/usb: WARNING: source write-protected, mounted read-only.
```



```
┌──(root㉿kali)-[/mnt/usb]
└─# ls
1  IMG_5609.JPG  IMG_5627.JPG  IMG_5753.JPG  IMG_6002.JPG  IMG_8064.JPG  text2.rar
```

Mamy dostęp do plików

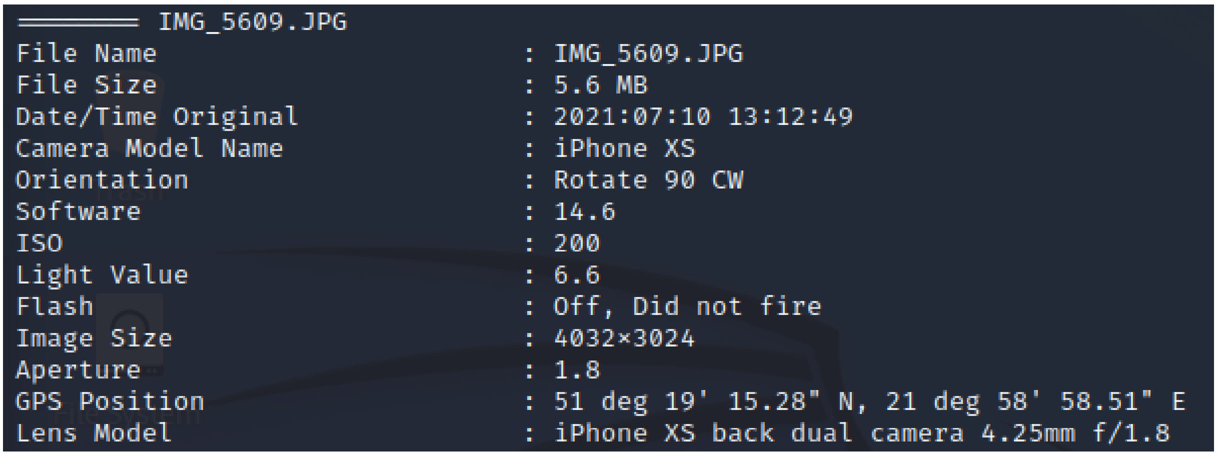


```
┌──(root㉿kali)-[/mnt/usb]
└─# exiftool IMG_5609.JPG
ExifTool Version Number         : 12.51
File Name                       : IMG_5609.JPG
Directory                       : .
File Size                       : 5.6 MB
File Modification Date/Time     : 2021:07:10 09:12:50-04:00
File Access Date/Time           : 2021:10:02 20:00:00-04:00
File Inode Change Date/Time     : 2021:07:10 09:12:50-04:00
File Permissions                : -rwxr-xr-x
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : Apple
Camera Model Name               : iPhone XS
Orientation                     : Rotate 90 CW
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : 14.6
```

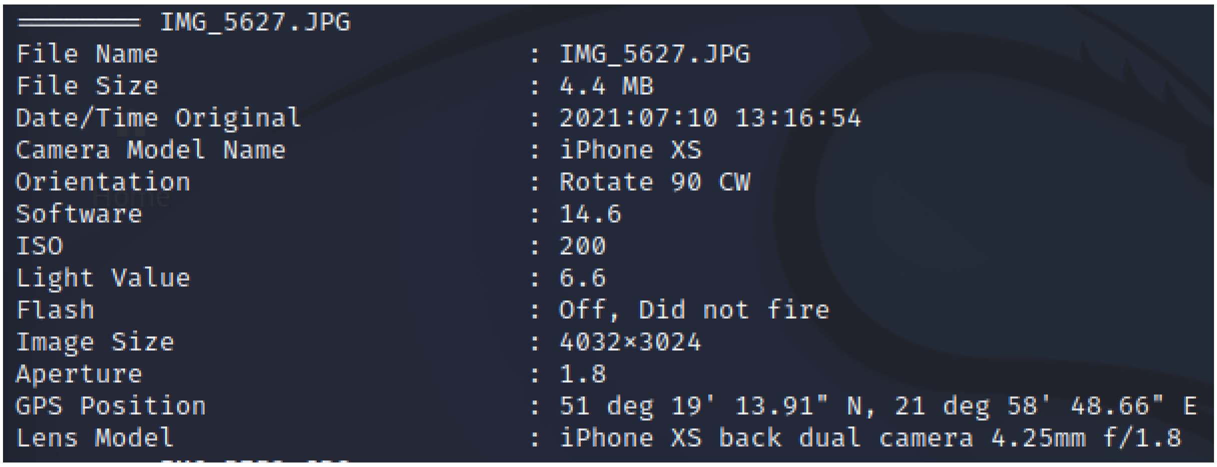
Aby wyczytać ze zdjęć interesujące, monotonne byłoby szukanie informacji ręcznie, dlatego skonstruowałem komendę przy użyciu TAGów:

exiftool -FileName -FileSize -DateTimeOriginal -Model -Orientation -Software -ISO -LightValue -Flash -ImageSize -Aperture -GPSPosition -LensModel IMG_*

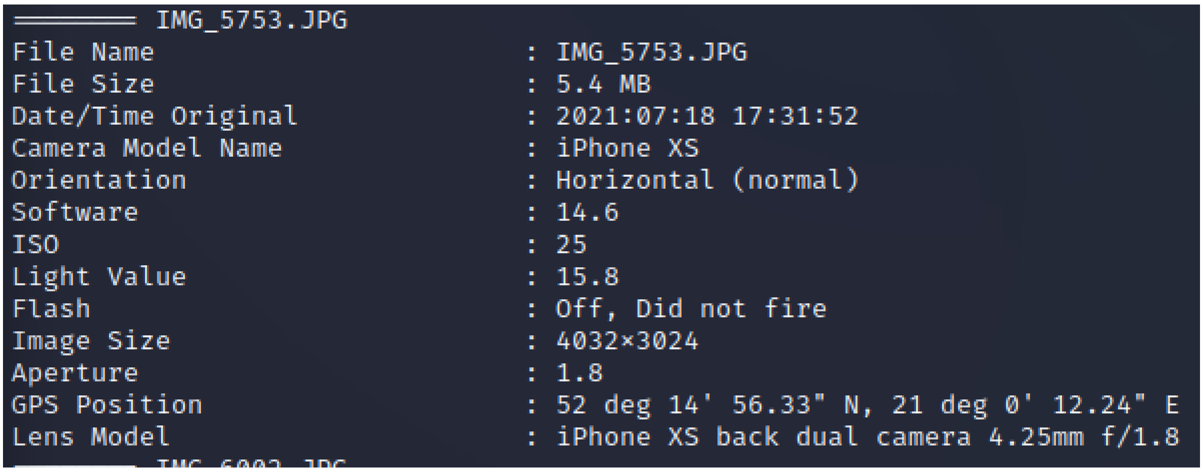
Powyższa komenda wypisuje jedynie wybrane TAGi ze wszystkich zdjęć znajdujących się w katalogu:



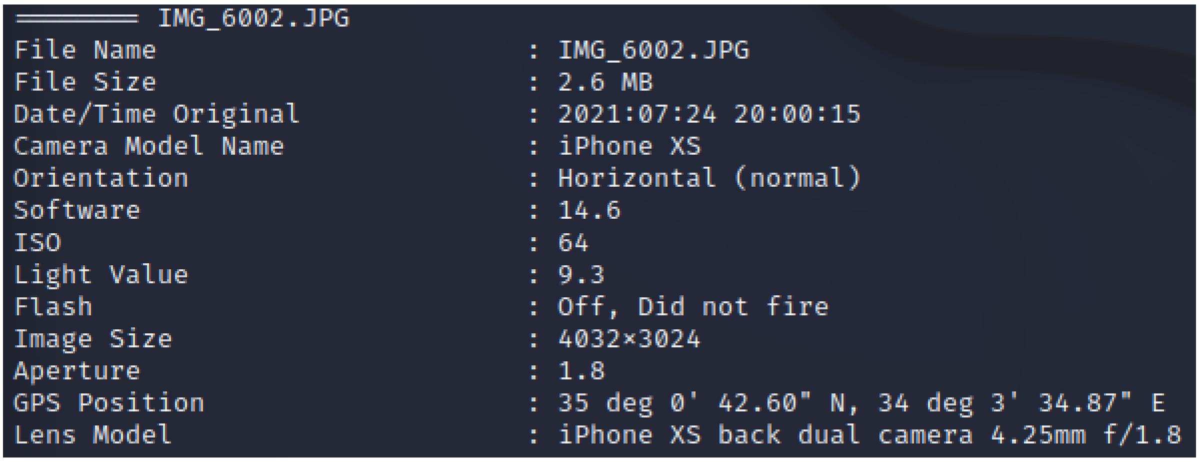
```
======== IMG_5609.JPG
File Name                       : IMG_5609.JPG
File Size                       : 5.6 MB
Date/Time Original              : 2021:07:10 13:12:49
Camera Model Name               : iPhone XS
Orientation                     : Rotate 90 CW
Software                        : 14.6
ISO                             : 200
Light Value                     : 6.6
Flash                           : Off, Did not fire
Image Size                      : 4032x3024
Aperture                        : 1.8
GPS Position                    : 51 deg 19' 15.28" N, 21 deg 58' 58.51" E
Lens Model                      : iPhone XS back dual camera 4.25mm f/1.8
```



```
======== IMG_5627.JPG
File Name                       : IMG_5627.JPG
File Size                       : 4.4 MB
Date/Time Original              : 2021:07:10 13:16:54
Camera Model Name               : iPhone XS
Orientation                     : Rotate 90 CW
Software                        : 14.6
ISO                             : 200
Light Value                     : 6.6
Flash                           : Off, Did not fire
Image Size                      : 4032×3024
Aperture                        : 1.8
GPS Position                    : 51 deg 19' 13.91" N, 21 deg 58' 48.66" E
Lens Model                      : iPhone XS back dual camera 4.25mm f/1.8
```



```
======== IMG_5753.JPG
File Name                       : IMG_5753.JPG
File Size                       : 5.4 MB
Date/Time Original              : 2021:07:18 17:31:52
Camera Model Name               : iPhone XS
Orientation                     : Horizontal (normal)
Software                        : 14.6
ISO                             : 25
Light Value                     : 15.8
Flash                           : Off, Did not fire
Image Size                      : 4032×3024
Aperture                        : 1.8
GPS Position                    : 52 deg 14' 56.33" N, 21 deg 0' 12.24" E
Lens Model                      : iPhone XS back dual camera 4.25mm f/1.8
```

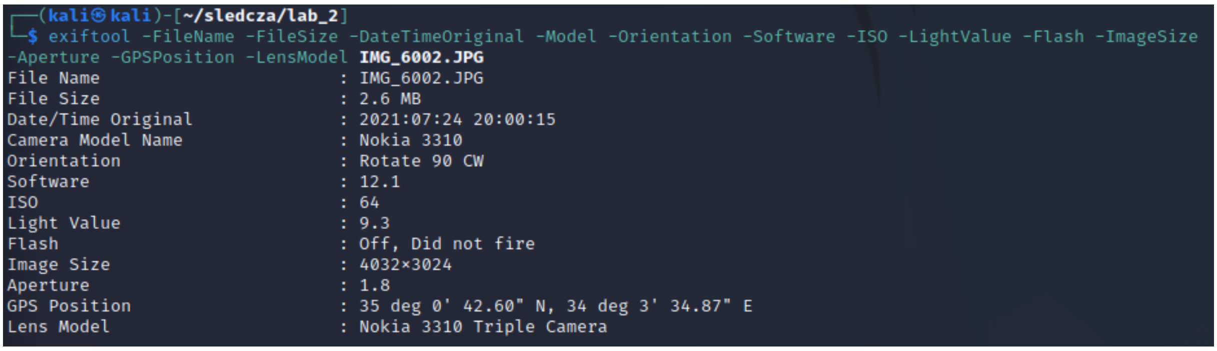


```
======== IMG_6002.JPG
File Name                       : IMG_6002.JPG
File Size                       : 2.6 MB
Date/Time Original              : 2021:07:24 20:00:15
Camera Model Name               : iPhone XS
Orientation                     : Horizontal (normal)
Software                        : 14.6
ISO                             : 64
Light Value                     : 9.3
Flash                           : Off, Did not fire
Image Size                      : 4032×3024
Aperture                        : 1.8
GPS Position                    : 35 deg 0' 42.60" N, 34 deg 3' 34.87" E
Lens Model                      : iPhone XS back dual camera 4.25mm f/1.8
```

Zmiana wartości za pomocą komendy dla pliku IMG_6002.JPG:

exiftool -Model="Nokia 3310" -Software="12.1" -Orientation="Rotate 90 CW" -LensModel="Nokia 3310 Triple Camera" -ImageSize="1920x1080" IMG_6002.JPG

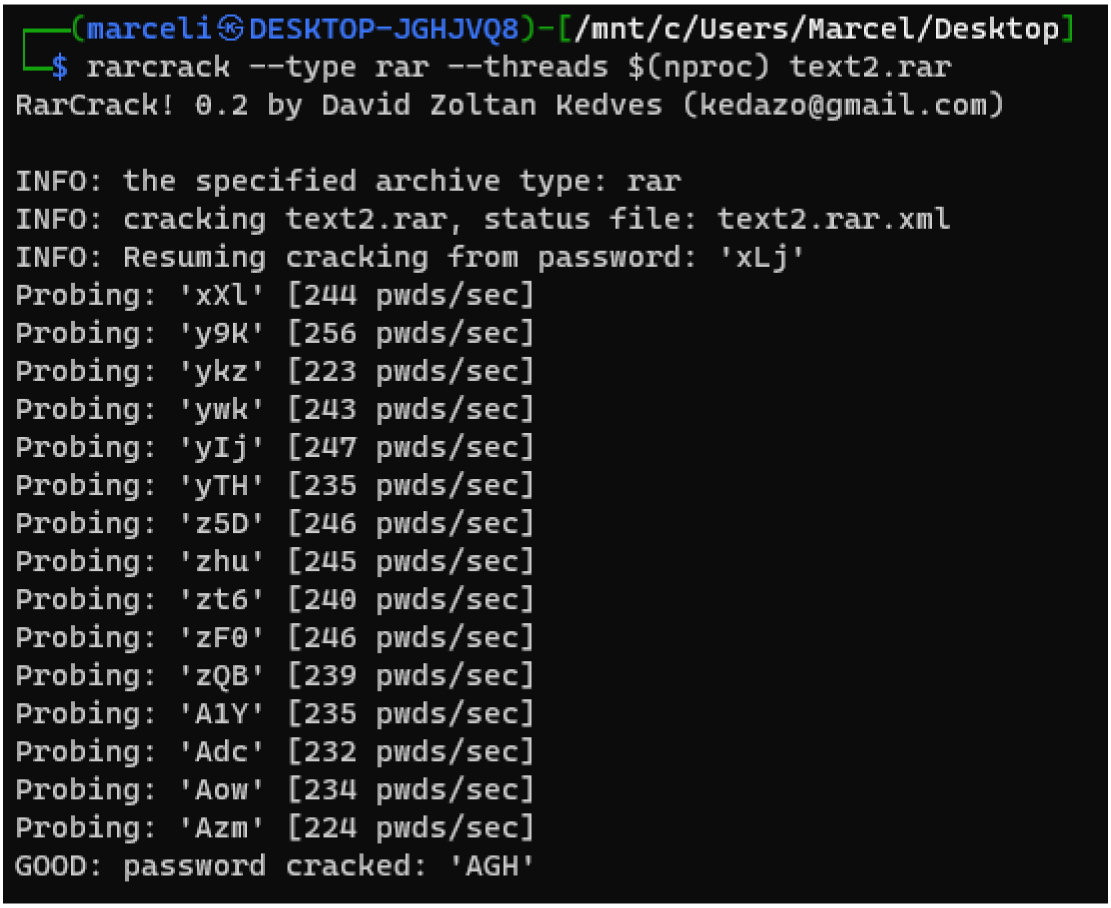
Po wypisaniu metadanych:



```
┌──(kali㉿kali)-[~/sledcza/lab_2]
└─$ exiftool -FileName -FileSize -DateTimeOriginal -Model -Orientation -Software -ISO -LightValue -Flash -ImageSize
-Aperture -GPSPosition -LensModel IMG_6002.JPG
File Name                       : IMG_6002.JPG
File Size                       : 2.6 MB
Date/Time Original              : 2021:07:24 20:00:15
Camera Model Name               : Nokia 3310
Orientation                     : Rotate 90 CW
Software                        : 12.1
ISO                             : 64
Light Value                     : 9.3
Flash                           : Off, Did not fire
Image Size                      : 4032x3024
Aperture                        : 1.8
GPS Position                    : 35 deg 0' 42.60" N, 34 deg 3' 34.87" E
Lens Model                      : Nokia 3310 Triple Camera
```

Łamanie hasła

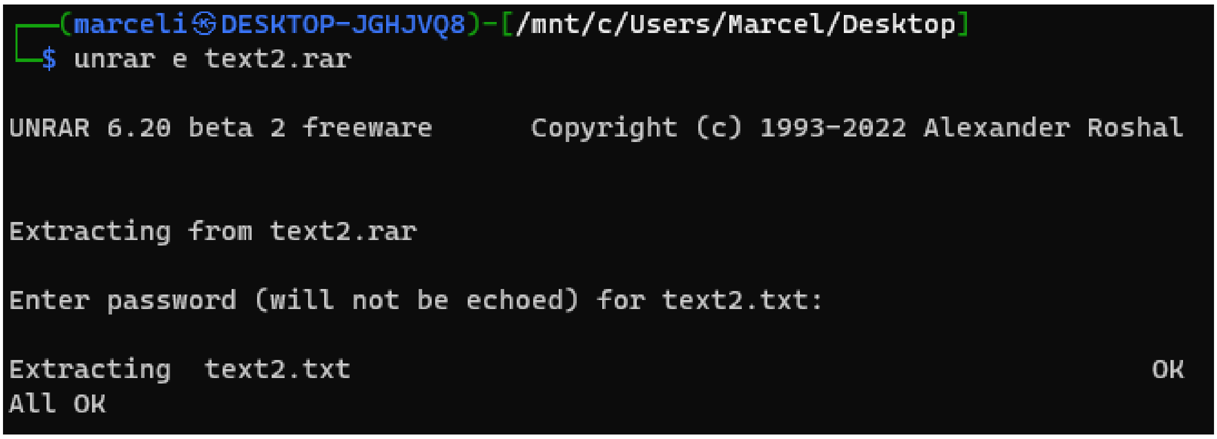
Po skopiowaniu pliku z usb do osobnego folderu użyłem komendy rarcrack do złamania hasła pliku rar:



```
┌──(marceli㉿DESKTOP-JGHJVQ8)-[/mnt/c/Users/Marcel/Desktop]
└─$ rarcrack --type rar --threads $(nproc) text2.rar
RarCrack! 0.2 by David Zoltan Kedves (kedazo@gmail.com)

INFO: the specified archive type: rar
INFO: cracking text2.rar, status file: text2.rar.xml
INFO: Resuming cracking from password: 'xLj'
Probing: 'xXl' [244 pwds/sec]
Probing: 'y9K' [256 pwds/sec]
Probing: 'ykz' [223 pwds/sec]
Probing: 'ywk' [243 pwds/sec]
Probing: 'yIj' [247 pwds/sec]
Probing: 'yTH' [235 pwds/sec]
Probing: 'z5D' [246 pwds/sec]
Probing: 'zhu' [245 pwds/sec]
Probing: 'zt6' [240 pwds/sec]
Probing: 'zF0' [246 pwds/sec]
Probing: 'zQB' [239 pwds/sec]
Probing: 'A1Y' [235 pwds/sec]
Probing: 'Adc' [232 pwds/sec]
Probing: 'Aow' [234 pwds/sec]
Probing: 'Azm' [224 pwds/sec]
GOOD: password cracked: 'AGH'
```

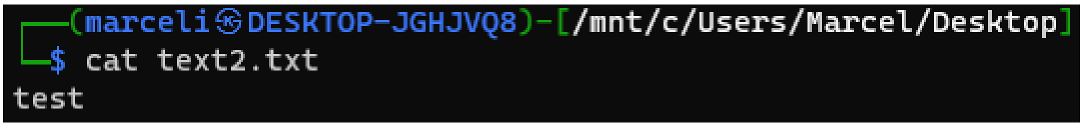
Hasło to AGH

Rozpakowujemy archiwum



```
┌──(marceli㉿DESKTOP-JGHJVQ8)-[/mnt/c/Users/Marcel/Desktop]
└─$ unrar e text2.rar

UNRAR 6.20 beta 2 freeware      Copyright (c) 1993-2022 Alexander Roshal


Extracting from text2.rar

Enter password (will not be echoed) for text2.txt:

Extracting  text2.txt                                                 OK
All OK
```

Treść pliku:



```
┌──(marceli㉿DESKTOP-JGHJVQ8)-[/mnt/c/Users/Marcel/Desktop]
└─$ cat text2.txt
test
```