Raport – Laboratorium nr 2 – Szymon Szkarłat

Zadanie 1. – Montowanie pliku .E01 jako nośnika pamięci przy wykorzystaniu pakietu EwfTools.
Zainstalowanie narzędzia EwfTools.

```
┌──(szymon㉿kali)-[~]
└─$ sudo apt install libewf-dev ewf-tools
[sudo] password for szymon:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
libewf-dev is already the newest version (20140814-1).
ewf-tools is already the newest version (20140814-1).
0 upgraded, 0 newly installed, 0 to remove and 1344 not upgraded.
```

1. Utworzenie pliku tmp w katalogu /mnt

```
┌──(root㉿kali)-[/mnt]
└─# ls -la
total 8
drwxr-xr-x  2 root root 4096 Oct 25 18:58 .
drwxr-xr-x 19 root root 4096 May 10 16:16 ..
-rw-r--r--  1 root root    0 Oct 25 18:58 tmp
```

2. Logowanie na konto roota

```
┌──(root㉿kali)-[/mnt]
└─# sudo -s
┌──(root㉿kali)-[/mnt]
└─#
```

3. Montowanie pliku z rozszerzeniem E01przy pomocy polecenia ewfmount plik.E01 /mnt/tmp

```
┌──(root㉿szymon)-[/home/szymon]
└─# ewfmount USB_4GB_Kingston.E01 /mnt/tmp
ewfmount 20140814


┌──(root㉿szymon)-[/home/szymon]
└─# ls -la /mnt/tmp/ewf1
-r--r--r-- 1 root root 3881828352 10-25 21:22 /mnt/tmp/ewf1
```

Sprawdzenie praw dostępu za pomocą komendy ls -la /mnt/tmp/ewf1

4. Początek sektora z danymi to 128, a wielkość sektora to 512 bajtów

```
┌──(root㉿szymon)-[/home/szymon]
└─# mmls /mnt/tmp/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 (0x0c)
```

5. Polecenie

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

6. Poleceniem df -k ujawniamy zamontowany obraz w /dev/loop0 (/mnt/tmp).

Dodatkowo, aby zamontować obraz używam polecenia: mount /dev/loop0 /media/kali
Na wcześniej utworzony za pomocą mkdir nowym folderze kali.

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

┌──(root㉿szymon)-[/home/szymon]
└─# df -k
System plików     1K-bl    użyte dostępne %uż. zamont. na
udev             4010352        0   4010352   0% /dev
tmpfs             810188     1468    808720   1% /run
/dev/sda1       29801344 12796360 15465812  46% /
tmpfs            4050936        0   4050936   0% /dev/shm
tmpfs               5120        0      5120   0% /run/lock
tmpfs             810184       80    810104   1% /run/user/1000
/dev/loop0       3787056    34744   3752312   1% /media/kali
```

Zadanie 2. – Wykonanie analizy zdjęć znajdujących się w zamontowanym obrazie (tmp – nazwa katalogu). Zmodyfikowano metadane znajdujące się w plikach jpeg.

```
┌──(root㉿szymon)-[/media/kali]
└─# ls -a
.   1              IMG_5627.JPG  IMG_6002.JPG  .Spotlight-V100
..  IMG_5609.JPG   IMG_5753.JPG  IMG_8064.JPG  text2.rar
```

Wybieram zdjęcia IMG_6002.JPG, IMG_5609.JPG, IMG_5753.JPG, IMG_8064.JPG
Wynik komendy exiftool

```
┌──(root㉿szymon)-[/media/kali]
└─# exiftool IMG_8064.JPG
ExifTool Version Number         : 12.67
File Name                       : IMG_8064.JPG
Directory                       : .
File Size                       : 6.5 MB
File Modification Date/Time     : 2021:08:07 19:57:34+02:00
File Access Date/Time           : 2021:10:03 02:00:00+02:00
File Inode Change Date/Time     : 2021:08:07 19:57:34+02:00
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
Modify Date                     : 2021:08:07 17:57:34
Host Computer                   : iPhone XS
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/518
F Number                        : 1.8
```

Zdjęcie: IMG_6002.JPG
Rozmiar: 2.6 MB
Data utworzenia: 2021:07:24 20:00:15
Urządzenie wykonujące zdjęcie: Apple iPhone XS
Orientacje: pozioma (normalna)
Wersja oprogramowania: 14.6
Wartość parametru ISO: 64
Ustawienie światła: 1/121
Flash: nie został użyty, wyłączony
Rozdzielczość fotografii: 4032x3024
Przesłona urządzenia wykonującego zdjęcie: f/1.8
Lokalizacja wykonania zdjęcia na podstawie GPS: Cypr
Liczba obiektów: Dwa obiekty (iPhone XS back dual camera 4.25mm f/1.8)

Zdjęcie: IMG_5609.JPG
Rozmiar: 5.6 MB
Data utworzenia: 2021:07:10 13:12:49
Urządzenie wykonujące zdjęcie: Apple iPhone XS
Orientacje: Obrócone o 90 stopni (Rotate 90 CW)
Wersja oprogramowania: 14.6
Wartość parametru ISO: 200
Ustawienie światła: 1/60
Flash: nie został użyty, wyłączony
Rozdzielczość fotografii: 4032x3024
Przesłona urządzenia wykonującego zdjęcie: f/1.8
Lokalizacja wykonania zdjęcia na podstawie GPS: Wąwóz w Kazimierzu Dolnym
Liczba obiektów: Dwa obiekty (iPhone XS back dual camera 4.25mm f/1.8)

Zdjęcie: IMG_5753.JPG:
Rozmiar: 5.4 MB
Data utworzenia: 2021:07:18 17:31:52
Urządzenie wykonujące zdjęcie: Apple iPhone XS
Orientacje: Pozioma (normalna)
Wersja oprogramowania: 14.6
Wartość parametru ISO: 25
Ustawienie światła: 1/4274
Flash: nie został użyty, wyłączony
Rozdzielczość fotografii: 4032x3024
Przesłona urządzenia wykonującego zdjęcie: f/1.8
Lokalizacja wykonania zdjęcia na podstawie GPS: Ogród Krasińskich Warszawa
Liczba obiektów: Dwa obiekty (iPhone XS back dual camera 4.25mm f/1.8)

Zdjęcie: IMG_8064.JPG
Rozmiar: 6.5 MB
Data utworzenia: 2021:08:07 17:57:34
Urządzenie wykonujące zdjęcie: Apple iPhone XS

Orientacje: Obrócone o 90 stopni (Rotate 90 CW)
Wersja oprogramowania: 14.6
Wartość parametru ISO: 25
Ustawienie światła: 1/518
Flash: nie został użyty, auto
Rozdzielczość fotografii: 4032x3024
Przesłona urządzenia wykonującego zdjęcie: f/1.8
Lokalizacja wykonania zdjęcia na podstawie GPS: Ogród Krasińskich Warszawa
Liczba obiektów: Dwa obiekty (iPhone XS back dual camera 4.25mm f/1.8)

Proszę o wybranie 5 dowolnych wartości oraz ich retusz (np. zmiana lokalizacji z oryginalnego na własną, zmiana nazwy urządzenia, innych wartości).

Pierwszym krokiem jest skopiowanie zdjęcia do innego folderu. Kolejny krok to modyfikacja zdjęć

```
┌──(root㉿szymon)-[/media/kali]
└─# cp IMG_6002.JPG /home/szymon

┌──(root㉿szymon)-[/media/kali]
└─# cd /home/szymon
```

```
┌──(root㉿szymon)-[/home/szymon]
└─# ls -a
.                .gnupg          .sudo_as_admin_successful
..               .ICEauthority   Szablony
.bash_logout     IMG_6002.JPG    USB_4GB_Kingston.E01
.bashrc          .java           Wideo
```

1. Zmiana nazwy modelu:

```
┌──(root㉿szymon)-[/home/szymon]
└─# exiftool -Make="LG" IMG_6002.JPG
    1 image files updated

┌──(root㉿szymon)-[/home/szymon]
└─# exiftool -Make IMG_6002.JPG
Make                            : LG
```

2. Zmiana orientacji na pionową

```
┌──(root㉿szymon)-[/home/szymon]
└─# exiftool -Orientation="Vertical" IMG_6002.JPG
    1 image files updated

┌──(root㉿szymon)-[/home/szymon]
└─# exiftool -Orientation IMG_6002.JPG
Orientation                     : Mirror vertical
```

3. Zmiana opisu na: *Zmiany w pliku*

```
┌──(root㉿szymon)-[/home/szymon]
└─# exiftool -ImageDescription="Zmiany w pliku" IMG_6002.JPG
    1 image files updated

┌──(root㉿szymon)-[/home/szymon]
└─# exiftool -ImageDescription IMG_6002.JPG
Image Description               : Zmiany w pliku
```

4. Zmiana marki aparatu (obiektywu) na: Nokia

```
┌──(root㉿szymon)-[/home/szymon]
└─# exiftool -LensMake="Nokia" IMG_6002.JPG
    1 image files updated

┌──(root㉿szymon)-[/home/szymon]
└─# exiftool -LensMake IMG_6002.JPG
Lens Make                       : Nokia
```

5. Zmiana lokalizacji na miasto w Turcji

```
┌──(root㉿szymon)-[/home/szymon]
└─# exiftool -GPSLatitude="38.88351349953744" -GPSLongitude="33.9798926275850
66" IMG_6002.JPG
    1 image files updated

┌──(root㉿szymon)-[/home/szymon]
└─# exiftool -GPSLatitude -GPSLongitude IMG_6002.JPG
GPS Latitude                    : 38 deg 53' 0.65" N
GPS Longitude                   : 33 deg 58' 47.61" E
```

Zadanie 3. – Wykorzystując język programowania Python sporządzić skrypt, który umożliwi wyświetlenie z konsoli Linuxa podstawowe informacje z metadanych pliku jpg (np. czas wykonania zdjęcia)

Skrypt utworzony w języku Python, w edytorze VIM

```python
#!/usr/bin/env python

from __future__ import print_function
import argparse
from datetime import datetime as dt
import os
import sys

from PIL import Image
from PIL.ExifTags import TAGS

def get_jpg_metadata(filePath):
    try:
        with Image.open(filePath) as img:
            exifData = img.getexif()
            if exifData:
                print(f"Metadata for file {filePath}")
                for tagID in exifData:
                    tag = TAGS.get(tagID, tagID)
                    data = exifData.get(tagID)
                    if isinstance(data, bytes):
                        data = data.decode()
                    print(f"{tag:25}: {data}")
            else:
                print("No EXIF matadata found in the file.")
    except Exception as error:
        print(f"Error: {error}")

if __name__ == "__main__":
    parser = argparse.ArgumentParser(description="Print metadata from a JPG file.")
    parser.add_argument("filePath", help="Path to the JPG file")
    args = parser.parse_args()

    get_jpg_metadata(args.filePath)
```

Wynik działania programu, na przykładzie zdjęcia IMG_6002.JPG

```
┌──(root㉿szymon)-[/home/szymon]
└─# vim jpg_printer.py

┌──(root㉿szymon)-[/home/szymon]
└─# ./jpg_printer.py IMG_6002.JPG
Metadata for file IMG_6002.JPG
GPSInfo                 : 2136
ResolutionUnit          : 2
ExifOffset              : 248
ImageDescription        : Zmiany w pliku
Make                    : LG
Model                   : iPhone XS
Software                : 14.6
Orientation             : 4
DateTime                : 2021:07:24 20:00:15
YCbCrPositioning        : 1
XResolution             : 72.0
YResolution             : 72.0
HostComputer            : iPhone XS
```

Zadanie 4. - W trakcie analizy śledczej może pojawić się potrzeba przełamania zabezpieczenia w postaci hasła np. rar. Przy użyciu programu Rarcrack można obejść proste zabezpieczenia i pozyskać dane z archiwum.

Instalowanie rarcrack

```
┌──(root㉿szymon)-[/home/szymon]
└─# sudo apt install rarcrack
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności... Gotowe
Odczyt informacji o stanie... Gotowe
Zostaną zainstalowane następujące NOWE pakiety:
  rarcrack
0 aktualizowanych, 1 nowo instalowanych, 0 usuwanych i 1411 nieaktualizowanyc
```

Pierwsza próba

```
┌──(root㉿szymon)-[/home/szymon]
└─# rarcrack --type rar 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
Probing: '0J' [35 pwds/sec]
Probing: '2s' [35 pwds/sec]
Probing: '4c' [36 pwds/sec]
Probing: '5P' [33 pwds/sec]
Probing: '7w' [35 pwds/sec]
Probing: '9e' [35 pwds/sec]
Probing: 'aV' [35 pwds/sec]
Probing: 'cB' [34 pwds/sec]
```

Pierwsza próba się nie powiodła, kolejno zmieniłem dane konfiguracyjne w pliku, usunąłem z niego cyfry, pozostawiając w nim jedynie małe i duże litery.

```
Plik  Działania  Edycja  Widok  Pomoc
<?xml version="1.0" encoding="UTF-8"?>
<rarcrack>
  <abc>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ</abc>
  <current>AGL</current>
  <good_password/>
</rarcrack>
```

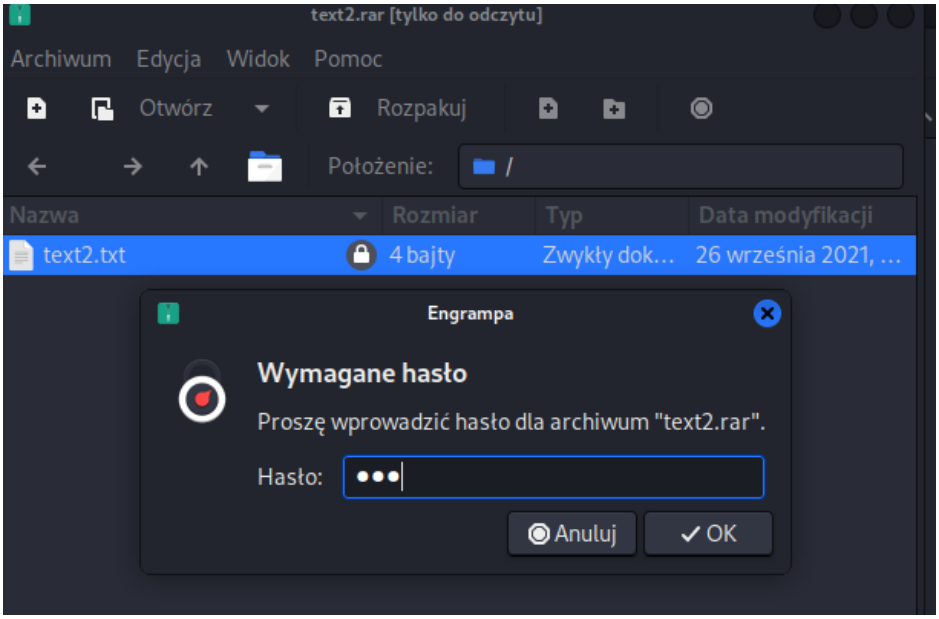
Uruchomiłem program jeszcze raz, startując od „aaa”

```
┌──(root㉿szymon)-[/home/szymon]
└─# rarcrack --type rar --threads 3 text2.rar
RarCrack! 0.2 by David Zoltan Kedves (kedazo@gmail.com)
```

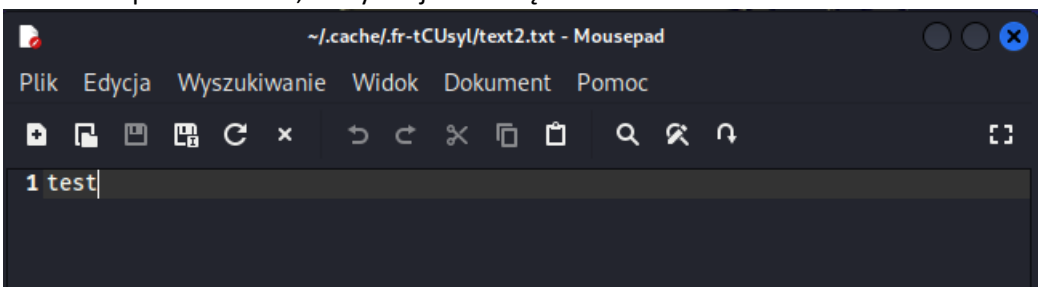
Po dłuższej chwili udało się metodą „brute force” znaleźć hasło, które brzmi: AGH

```
Probing: 'zaL' [92 pwds/sec]
Probing: 'zgq' [97 pwds/sec]
Probing: 'zlT' [96 pwds/sec]
Probing: 'zrv' [96 pwds/sec]
Probing: 'zwZ' [96 pwds/sec]
Probing: 'zCB' [96 pwds/sec]
Probing: 'zIh' [97 pwds/sec]
Probing: 'zNM' [97 pwds/sec]
Probing: 'zTs' [97 pwds/sec]
Probing: 'zYW' [96 pwds/sec]
Probing: 'Aez' [96 pwds/sec]
Probing: 'Akc' [96 pwds/sec]
Probing: 'ApG' [96 pwds/sec]
Probing: 'Avj' [96 pwds/sec]
Probing: 'AAO' [97 pwds/sec]
Probing: 'AGp' [95 pwds/sec]
GOOD: password cracked: 'AGH'
```

Wprowadzam hasło, które należy podać przy otwieraniu pliku test2.rar, tj. AGH



Zawartość pliku text2.txt, który znajdował się w archiwum text2.rar.



Zadanie 5. – Odmontuj wirtualny nośnik /dev/loop0

Przy pomocy polecenia umount /dev/loop) odmontowuję obraz dysku

```
┌──(root㉿szymon)-[/home/szymon]
└─# df -k
System plików     1K-bl    użyte dostępne %uż. zamont. na
udev             4010352        0  4010352   0% /dev
tmpfs             810188     1476   808712   1% /run
/dev/sda1       29801344 12804288 15457884  46% /
tmpfs            4050936        0  4050936   0% /dev/shm
tmpfs               5120        0     5120   0% /run/lock
tmpfs             810184       88   810096   1% /run/user/1000
/dev/loop0       3787056    34744  3752312   1% /media/kali

┌──(root㉿szymon)-[/home/szymon]
└─# umount /dev/loop0

┌──(root㉿szymon)-[/home/szymon]
└─# df -k
System plików     1K-bl    użyte dostępne %uż. zamont. na
udev             4010352        0  4010352   0% /dev
tmpfs             810188     1476   808712   1% /run
/dev/sda1       29801344 12804292 15457880  46% /
tmpfs            4050936        0  4050936   0% /dev/shm
tmpfs               5120        0     5120   0% /run/lock
tmpfs             810184       88   810096   1% /run/user/1000
```

Nie ma obrazu dysku. Potwierdzenie w „lsblk”. Nie żadnych MOUNTPOINTS.

```
┌──(root㉿szymon)-[/home/szymon]
└─# lsblk -a
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0    7:0    0  3,6G  1 loop
```