

# Informatyka śledcza

## Laboratorium nr 2

### Spis treści

- Zadanie 1 – Montowanie pliku .E01 przy pomocy narzędzia ewfmount.
- Zadanie 2 – Analiza zamontowanego obrazu przy pomocy pakietu ExifTool.
- Zadanie 3 – Pozyskiwanie danych z pliku przy pomocy języka programowania Python 3.
- Zadanie 4 – Przełamanie hasła (.rar)
- Zadanie 5 – Odmontowanie wirtualnego nośnika.

### Wstęp

To laboratorium ma na celu wykorzystanie w praktyce narzędzia ewfmount do zamontowania wirtualnego nośnika z pliku .E01, pobranego z poprzednich zajęć. W przypadku poprawnego wykorzystania narzędzia z pakietu Ewf-Tools ujrzymy zawartość nośnika wraz ze wszystkimi znajdującymi się wewnątrz plikami. Mając do nich dostęp jesteśmy w stanie przy użyciu pakietu ExifTool pozyskać informacje z plików graficznych i odpowiedzieć na kilka niżej zadanych pytań. W ramach tego laboratorium poznamy metody zniekształcania metadanych zawartych wewnątrz plików .jpeg oraz zapoznamy się z atakiem typu brute-force, który pomoże nam ujawnić hasło z pliku .rar.

### Wykorzystywane narzędzia w trakcie laboratorium:

1. *EwfTools (sudo apt install libewf-dev ewf-tools)*
3. *Rarcrack*
4. *Python*

### Zadanie 1 – Montowanie pliku .E01 jako nośnik pamięci przy wykorzystaniu pakietu EwfTools.

W tym zadaniu wykorzystaj narzędzie *ewfmount* do zamontowania pliku .E01 jako nośnik danych, który będzie widziany przez system tak samo jak podpięty pendrive. W trakcie zadania wykorzystaj i zmodyfikuj polecenia:

1. Utwórz plik *tmp* w katalogu */mnt*.
2. Zaloguj się na roota (*sudo -s*).

```
(kali@kali) - [~/Desktop/IMG]
$ sudo -s
[sudo] password for kali:
(root@kali) - [/home/kali/Desktop/IMG]
```

3. Zamontuj plik .E01 w systemie Linux.

- Wykonaj polecenie:

`ewfmount plik.E01 /mnt/tmp`

- Sprawdź prawa dostępu do pliku:

`ls -la /mnt/tmp/ewf1`

- Wykonaj polecenie `mmls` na pliku znajdującym się w katalogu `/mnt/tmp/ewf1`, w celu sprawdzenia startowej partycji z danymi. Zapamiętaj wielkość sektorów.

- Wykonaj polecenie: `losetup -r -o [(początek sektora z danymi) * (wielkość sektora)] /dev/loop0 /mnt/tmp/ewf1`

W tej chwili powinien pokazać się zamontowany obraz pendriva w „Devices”.

Polecenie `df -k` ujawni zamontowany obraz w `/dev/loop0` (kali/USB DISK).

```
(root@kali) - [/home/kali/Desktop/IMG]
# df -k
Filesystem      1K-blocks      Used Available Use% Mounted on
udev             2989852         0    2989852   0% /dev
tmpfs             605204         1208     603996   1% /run
/dev/sda1       154785160    115247880    31601792  79% /
tmpfs             3026012        16048     3009964   1% /dev/shm
tmpfs              5120           0         5120   0% /run/lock
tmpfs             605200         68      605132   1% /run/user/1000
/dev/loop0       3787056       34744     3752312   1% /media/kali/USB DISK
```

**Zadanie 2 – Wykonaj analizę zdjęć znajdujących się w zamontowanym obrazie (USB DISK). Zmodyfikuj metadane znajdujące się w plikach jpeg.**

Do zrealizowania tego zadania student musi posiadać dostęp do danych zawartych w „USB DISK”. W przypadku, gdy wykorzystywany system Linux nie posiada dostępu do narzędzia Exif, należy doinstalować niezbędne biblioteki.

```
(kali@kali) - [/media/kali/USB DISK]
$ exiftool
Command 'exiftool' not found, but can be installed with:
sudo apt install libimage-exiftool-perl
Do you want to install it? (N/y)y
sudo apt install libimage-exiftool-perl
[sudo] password for kali:
Reading package lists... Done
```

Mając dostęp do polecenia `exiftool` zbadaj 4 losowe zdjęcia z zamontowanego obrazu i odpowiedz na pytania:

- Jakiego mają rozmiary?
- Kiedy zostały utworzone?
- Jakiego urządzenia wykonało badane zdjęcie?
- Jaka była orientacja urządzenia w trakcie wykonywania fotografii (*Rotate:X:Y*)?
- Proszę o podanie wersji oprogramowania.
- Ile wynosi parametr ISO?
- Podaj ustawienie światła.
- Czy w trakcie robienia zdjęcia został użyty flash?
- Ile wynosi rozdzielczość fotografii?
- Jaką przesłonę ma urządzenie wykonujące zdjęcie?
- Gdzie zostało zrobione to zdjęcie?
- Ile obiektów posiada urządzenie?
- Proszę o wybranie 5 dowolnych wartości oraz ich retusz (np. zmiana lokalizacji z oryginalnego na własną, zmiana nazwy urządzenia, innych wartości).

**Zadanie 3 – Wykorzystując język programowania Python 3 sporządź prosty skrypt, który umożliwi wyświetlenie z konsoli linuxa podstawowych informacji z metadanych pliku jpg (np. czas wykonania zdjęcia).**

```
GNU nano 5.4
from __future__ import print_function
import argparse
from datetime import datetime as dt
import os
import sys
```

Pomocne importy do zadania.

**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.**

- Proszę o pobranie i zainstalowanie programu Rarcrack:

```
(kali@kali) - [/media/kali/USB_DISK1]
$ rarcrack
Command 'rarcrack' not found, but can be installed with:
sudo apt install rarcrack
Do you want to install it? (N/y)y
sudo apt install rarcrack
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  rarcrack
0 upgraded, 1 newly installed, 0 to remove and 327 not upgraded.
Need to get 17.3 kB of archives.
After this operation, 50.2 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 rarcrack amd64 0.2-1+b1 [17.3 kB]
Fetched 17.3 kB in 1s (25.6 kB/s)
```

- Wykorzystując ww. program odzyskaj hasło z pliku *text2.rar* (przy pomocy metody *brute force*).



- Utwórz raport z laboratorium zamieszczając w nim zrzuty ekranów ujawniające hasło do pliku oraz wyciągniętą zawartość archiwum.

**Zadanie 5 – Odmontuj wirtualny nośnik */dev/loop0*.**

- Przy użyciu programu *EwffTools* odmontuj zamontowany obraz dysku. Zamieść zrzut ekranu z przeprowadzonej procedury.

**Rozwiązania zadań muszą zawierać zrzuty ekranów ze wszystkich wykonanych elementów oraz szczegółowy opis uzyskanych rezultatów.**