Informatyka Śledcza - Laboratorium 2

Magdalena Ślusarczyk

1 Montowanie pliku

1.1 Prawa do pliku

Dla każdego użytkownika możliwy jest tylko odczyt.

1.2 Informacje o obrazie

```
┌──(root💀kali)-[/home/kali/Desktop/SLEDCZA]
└─# 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)
```

2 Analiza zdjęć

2.1 IMG_5609

Rozmiar: 5.4MiB
Data utworzenia: 2021:07:18 17:31:52
Urządzenie: iPhone XS
Orientacja: Rotate 90 CW
Wersja oprogramowania: 14.6
ISO: 25
Ustawienie światła: 15.8
Flash: Off
Rozdzielczość: 4032 x 3024 px
Przesłona: 1.8
Miejsce: 51°19'15.3Ń 21°58'58.5Ę (Kazimierz Dolny)
Ilość obiektywów: 2

2.2 IMG_5753

Rozmiar: 5.1MiB
Data utworzenia: 2021:07:10 13:12:49
Urządzenie: iPhone XS
Orientacja: Horyzontalna
Wersja oprogramowania: 14.6
ISO: 200

Ustawienie światła: 6.6
Flash: Off
Rozdzielczość: 4032 x 3024 px
Przesłona: 1.8
Miejsce: 52°14'56.3Ń 21°00'12.2Ę (Muranów, Warszawa)
Ilość obiektywów: 2

2.3 IMG_6002

Rozmiar: 2.5MiB
Data utworzenia: 2021:07:24 20:00:15
Urządzenie: iPhone XS
Orientacja: Horyzontalna
Wersja oprogramowania: 14.6
ISO: 64
Ustawienie światła: 9.3
Flash: Off
Rozdzielczość: 4032 x 3024 px
Przesłona: 1.8
Miejsce: 35°00'42.6Ń 34°03'34.9Ę (Protaras, Cypr)
Ilość obiektywów: 2

2.4 IMG_8064

Rozmiar: 6.2MiB
Data utworzenia: 2021:08:07 17:57:34
Urządzenie: iPhone XS
Orientacja: Rotate 90 CW
Wersja oprogramowania: 14.6
ISO: 25
Ustawienie światła: 12.7
Flash: Auto, nie zapalił się
Rozdzielczość: 4032 x 3024 px
Przesłona: 1.8
Miejsce: 52°14'55.2Ń 21°00'14.7Ę (Muranów, Warszawa)
Ilość obiektywów: 2

2.5 Zmiana metadanych

```
┌──(root💀kali)-[/home/kali/Desktop/SLEDCZA]
└─# exiftool IMG_5609.JPG -make=Android -HostComputer=XiaomiMi9Lite -XResolution=300 -YResolution=300 -
Orientation=Horizontal
    1 image files updated

┌──(root💀kali)-[/home/kali/Desktop/SLEDCZA]
└─# exiftool IMG_5609.JPG -make -HostComputer -XResolution -YResolution -Orientation
Make                            : Android
Host Computer                   : XiaomiMi9Lite
X Resolution                    : 300
Y Resolution                    : 300
Orientation                     : Horizontal (normal)
```

3 Rarcrack

```
Probing: 'ADp' [57 pwds/sec]
Probing: 'AG4' [55 pwds/sec]
GOOD: password cracked: 'AGH'
```

4 Odmontowanie

```
┌──(root💀kali)-[/home/kali/Desktop/SLEDCZA]
└─# umount /dev/loop0                                                    1 ⚙

┌──(root💀kali)-[/home/kali/Desktop/SLEDCZA]
└─# losetup -f                                                           1 ⚙
/dev/loop0

┌──(root💀kali)-[/home/kali/Desktop/SLEDCZA]
└─# mount |grep tmp                                                      1 ⚙
udev on /dev type devtmpfs (rw,nosuid,relatime,size=2993760k,nr_inodes=748440,mode=755)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=605988k,mode=755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=605984k,nr_inodes=151496,mo
de=700,uid=1000,gid=1000)
/dev/fuse on /home/kali/Desktop/SLEDCZA/mnt/tmp type fuse (rw,nosuid,nodev,relatime,user_id=0
,group_id=0)

┌──(root💀kali)-[/home/kali/Desktop/SLEDCZA]
└─# umount ./mnt/tmp                                                     1 ⚙

┌──(root💀kali)-[/home/kali/Desktop/SLEDCZA]
└─# mount |grep tmp                                                      1 ⚙
udev on /dev type devtmpfs (rw,nosuid,relatime,size=2993760k,nr_inodes=748440,mode=755)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=605988k,mode=755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=605984k,nr_inodes=151496,mo
de=700,uid=1000,gid=1000)

┌──(root💀kali)-[/home/kali/Desktop/SLEDCZA]
└─#                                                                      1 ⚙
```