Zadanie 2

1. Jaka jest wartość skrótu dla funkcji haszującej md5 i sha-1?

```
[arek@fedora lab1] $ md5sum USB_4GB_Kingston.E01
b879553c628b3308d624372398d8302a  USB_4GB_Kingston.E01
```

```
[arek@fedora lab1] $ sha1sum USB_4GB_Kingston.E01
344aa2b0179e18ad94ddcc0e5cbfa0af663faba3  USB_4GB_Kingston.E01
```

1. W jakim przedziale sektorów znajduje się niealokowana pamięć?:

0000000000 - 0000000127

2. W której partycji znajdują się pliki systemowe?

Win95 FAT32 (0x0c) - numer 002

3. Proszę o podanie początku i końca sektora należącego do partycja Win95?

0000000128 - 0007581695

1. Jaki system plików zaczyna się w sektorze 0000000128 analizowanego pliku?

FAT32

2. Jaka jest wielkość sektora oraz klastra w badanym obszarze?

```
----------------------------------------------
Sector Size: 512
Cluster Size: 8192
Total Cluster Range: 2 - 473383
```

Sector Size: 512

Cluster Size: 8192

1. Wypisz wszystkie pliki głównego katalogu USB_4GB_Kingston.E01.

```
[arek@fedora lab1] $ fls -o 128 -f fat32 USB_4GB_Kingston.E01
r/r 3:  USB DISK    (Volume Label Entry)
d/d 6:  .Spotlight-V100
d/d * 8:        .fseventsd
d/d 9:  1
r/r 10: IMG_5609.JPG
r/r * 13:       ._IMG_5609.JPG
r/r 14: IMG_5627.JPG
r/r * 17:       ._IMG_5627.JPG
r/r 18: IMG_5753.JPG
r/r * 21:       ._IMG_5753.JPG
r/r 22: IMG_6002.JPG
r/r * 25:       ._IMG_6002.JPG
r/r 26: IMG_8064.JPG
r/r * 29:       ._IMG_8064.JPG
r/r 30: text2.rar
r/r * 32:       ._text2.rar
r/r * 34:       ._1
v/v 121185795:  $MBR
v/v 121185796:  $FAT1
v/v 121185797:  $FAT2
V/V 121185798:  $OrphanFiles
```

2. Wypisz wszystkie plik znajdujące się w folderze „1”.

```
[arek@fedora lab1] $ fls -o 128 -f fat32 -r USB_4GB_Kingston.E01 9
r/r 62725:      IMG_6110.JPG
r/r 62726:      IMG_5592.JPG
r/r 62727:      text.txt
```

1. Pod jaki numer sprawy podlega badany nośnik?

```
[arek@fedora lab1] $ ewfinfo -m USB_4GB_Kingston.E01
ewfinfo 20140608

EWF information
        File format:            EnCase 6
        Sectors per chunk:      64
        Error granularity:      64
        Compression method:     deflate
        Compression level:      good (fast) compression

Media information
        Media type:             removable disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      7581696
        Media size:             3.6 GiB (3881828352 bytes)

Digest hash information
        MD5:                    5df8f604967c556c810d21dd664ceae4
```

Case number: 001

2. Jaka jest nazwa osoby tworzącej obraz dysku?

Examiner name: Kali

3. Kiedy plik został utworzony?

Sun Oct 3 16:31:05 2021

4. Numer seryjny fizycznego dysku oraz nazwa modelu?

Serial number: 0D7117891080
Model: USB DISK 2.0

5. Wskaż format plików?

```
[arek@fedora lab1] $ ewfinfo -m USB_4GB_Kingston.E01
ewfinfo 20140608

EWF information
        File format:            EnCase 6
        Sectors per chunk:      64
        Error granularity:      64
        Compression method:     deflate
        Compression level:      good (fast) compression

Media information
        Media type:             removable disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      7581696
        Media size:             3.6 GiB (3881828352 bytes)

Digest hash information
        MD5:                    5df8f604967c556c810d21dd664ceae4
```

File format: EnCase 6

6. Proszę o podanie metody kompresji pliku?

Compression method: deflate

7. Jaka jest pełna wielkość badanego nośnika (w bajtach)?

3881828352 bytes

8. Jaki poziom kompresji został wskazany przy tworzeniu pliku?

Compression level: good (fast) compression

Zadanie 3

1. Wczytaj za pomocą polecenia mmls i podaj liczbę sektorów gpt_load_table.

1

```
load_pri:0:2    Start: 0   Size: 0  Type: 0
load_pri:0:3    Start: 0   Size: 0  Type: 0
bsd_load_table: Table Sector: 1
gpt_load_table: Sector: 1
gpt_load: 0  Starting Sector: 2048  End: 104447
gpt_load: 1  Starting Sector: 104448  End: 3092
gpt_load: 2  Starting Sector: 309248  End: 7188
gpt_load: 3  Starting Sector: 718848  End: 1058
gpt_load: 4  Starting Sector: 1058816  End: 109
gpt_load: 5  Starting Sector: 1091584  End: 117
gpt_load: 6  Starting Sector: 0  End: 0 Flag: 0
gpt_load: 7  Starting Sector: 0  End: 0 Flag: 0
gpt_load: 8  Starting Sector: 0  End: 0 Flag: 0
```

2. Proszę o podanie sektora startowego gpt_load: 0.

2048

3. Ile niealokowanych sektorów znajduję się w obrazie? Podaj ich sektory startowe oraz końcowe.

2

```
[arek@fedora lab1] $ mmls -A LAB_1.img
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
001:  -------   0000000000   0000002047   0000002048   Unallocated
010:  -------   0001173504   0001999999   0000826496   Unallocated
[arek@fedora lab1] $
```

0000002047 - 0000002048

0001999999 - 0000826496

4. Podaj ujawnione woluminy.

fat16

fat32

ntfs

ext4

swap

minix

```
[arek@fedora lab1] $ mmls -a LAB_1.img
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
004:  000       0000002048   0000104447   0000102400   fat16
005:  001       0000104448   0000309247   0000204800   fat32
006:  002       0000309248   0000718847   0000409600   ntfs
007:  003       0000718848   0001058815   0000339968   ext4
008:  004       0001058816   0001091583   0000032768   swap
009:  005       0001091584   0001173503   0000081920   minix
```

5. Wykorzystując polecenie mmstat wyświetl informacje tablicy partycji.

```
        -V: print the version
[arek@fedora lab1] $ mmstat -v LAB_1.img
tsk_img_open: Type: 0   NumImg: 1  Img1: LAB_1.img
aff_open: Error determining type of file: LAB_1.img
aff_open: Success
tsk_img_findFiles: LAB_1.img found
tsk_img_findFiles: 1 total segments found
raw_open: segment: 0  size: 1024000000  max offset: 1024000000  path: LAB_1.img
dos_load_prim: Table Sector: 0
raw_read: byte offset: 0 len: 65536
raw_read: found in image 0 relative offset: 0 len: 65536
raw_read_segment: opening file into slot 0: LAB_1.img
dos_load_prim_table: Testing FAT/NTFS conditions
load_pri:0:0    Start: 1   Size: 1999999  Type: 238
load_pri:0:1    Start: 0   Size: 0  Type: 0
load_pri:0:2    Start: 0   Size: 0  Type: 0
load_pri:0:3    Start: 0   Size: 0  Type: 0
bsd_load_table: Table Sector: 1
gpt_load_table: Sector: 1
gpt_load: 0  Starting Sector: 2048  End: 104447 Flag: 0
```

6. Przy wykorzystaniu narzędzia fsstat wyświetl informacje o woluminie „ntfs” oraz podaj „Volume Serial Number” oraz informacje o wersji („Version”).

Zadanie 4

```
Device     Boot Start       End   Sectors  Size Id Type
/dev/sdb1        32768 124735487 124702720 59.5G  7 HPFS/NTFS/exFAT
[arek@fedora lab1] $
```

```
Wipe sectors on read error (mimic EnCase like behavior) (yes, no) [no]: no

The following acquiry parameters were provided:
Image path and filename:                images.E01.E01
Case number:                            2
Description:                            First image acquired
Evidence number:                        23
Examiner name:                          Arek
Notes:                                  None
Media type:                             removable disk
Is physical:                            no
EWF file format:                        EnCase 6 (.E01)
Compression method:                     deflate
Compression level:                      fast
Acquiry start offset:                   0
Number of bytes to acquire:             29 KiB (30000 bytes)
Evidence segment file size:             1.4 GiB (1493172224 bytes)
Bytes per sector:                       512
Block size:                             64 sectors
Error granularity:                      64 sectors
Retries on read error:                  2
Zero sectors on read error:             no

Continue acquiry with these values (yes, no) [yes]: yes

Acquiry started at: Oct 06, 2022 12:11:49
This could take a while.

Acquiry completed at: Oct 06, 2022 12:11:49

Written: 30 KiB (31316 bytes) in 0 second(s).
MD5 hash calculated over data:          faae6665301a2eaa6b4ad7432ca40086
ewfacquire: SUCCESS
```

```
ewfverify 20140608

Verify started at: Oct 06, 2022 12:12:28
This could take a while.

Verify completed at: Oct 06, 2022 12:12:28

Read: 29 KiB (29696 bytes) in 0 second(s).

MD5 hash stored in file:                faae6665301a2eaa6b4ad7432ca40086
MD5 hash calculated over data:          2b4929e06f45983ed8e79665e0d00ae7
```