```
┌──(kali㉿kali)-[~/sledcza]
└─$ md5sum USB_4GB_Kingston.E01
b879553c628b3308d624372398d8302a  USB_4GB_Kingston.E01
```

Suma MD5: b879553c628b3308d624372398d8302a

```
┌──(kali㉿kali)-[~/sledcza]
└─$ sha1sum USB_4GB_Kingston.E01
344aa2b0179e18ad94ddcc0e5cbfa0af663faba3  USB_4GB_Kingston.E01
```

Suma SHA-1: 344aa2b0179e18ad94ddcc0e5cbfa0af663faba3

```
┌──(kali㉿kali)-[~/sledcza]
└─$ mmls USB_4GB_Kingston.E01
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)
```

Niealokowana pamięć na przedziale: 0000000000 – 0000000127

Pliki systemowe znajdują się na partycji 002

Partycja Win95 zaczyna się na 0000000128 i kończy na 0007581695

System plików na sektorze 0000000128: FAT32

Wielkość sektora: 512
Wielkość klastra: 8192

```
┌──(kali㉿kali)-[~/sledcza]
└─$ fls -o 128 -u USB_4GB_Kingston.E01
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
```

W katalogu głównym znajduje się 5 obrazów i 1 archiwum rar

```
┌──(kali㉿kali)-[~/sledcza]
└─$ fls -o 128 -u -r USB_4GB_Kingston.E01 | grep -v '+++'
r/r 3:  USB DISK    (Volume Label Entry)
d/d 6:  .Spotlight-V100
+ d/d 262:      Store-V2
++ d/d 520:     6F621758-5262-4AB9-BAD2-96DA8EDBAF70
+ r/r 265:      VolumeConfiguration.plist
d/d 9:  1
+ r/r 62725:    IMG_6110.JPG
+ r/r 62726:    IMG_5592.JPG
+ r/r 62727:    text.txt
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
```

W folderze 1 znajdują się 2 zdjęcia i 1 plik tekstowy

```
┌──(kali㉿kali)-[~/sledcza]
└─$ ewfinfo -d dm USB_4GB_Kingston.E01
ewfinfo 20140813

Acquiry information
        Case number:            001
        Examiner name:          Kali
        Evidence number:        001
        Acquisition date:       03/10/2021 10:31:05
        System date:            03/10/2021 10:31:05
        Operating system used:  Linux
        Software version used:  20140807
        Password:               N/A
        Model:                  USB DISK 2.0
        Serial number:          0D7117891080

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
```

Numer sprawy: 001
Nazwa osoby tworzącej dysk: kali
Plik został utworzony 03/10/2021/ 10:31:05
Numer seryjny dysku: 0D7117891080
Nazwa modelu: USB DISK 2.0
Format plików: EnCase 6
Metoda kompresji: deflate
Wielkość w bajtach: 3881828352 bytes
Poziom kompresji: good (fast) compression

```
┌──(kali㉿kali)-[~/sledcza]
└─$ mmls LAB_1.img
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

     Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Safety Table
001:  ------    0000000000   0000002047   0000002048   Unallocated
002:  Meta      0000000001   0000000001   0000000001   GPT Header
003:  Meta      0000000002   0000000033   0000000032   Partition Table
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
010:  ------    0001173504   0001999999   0000826496   Unallocated
```

Liczba sektorów: 1999999
Sektor startowy 000: 2048
Liczba niezalokowanych sektorów: 828544
Ujawnione woluminy: fat16 fat32 ntfs ext4 swap minix
Tablica partycji: gpt

```
┌──(kali㉿kali)-[~/sledcza]
└─$ fsstat -o 309248 LAB_1.img
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: 451AF24C771A6637
OEM Name: NTFS
Volume Name: NTFS
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 4
First Cluster of MFT Mirror: 25599
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 68
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 51198
Total Sector Range: 0 - 409598
```

Volume Serial Number: 451AF24C771A6637
Version: Windows XP

```
The following acquiry parameters were provided:
Image path and filename:                ~/sledcza/sandisk.E01
Case number:                            1
Description:
Evidence number:                        1
Examiner name:                          Marcel
Notes:
Media type:                             removable disk
Is physical:                            yes
EWF file format:                        EnCase 6 (.E01)
Compression method:                     deflate
Compression level:                      none
Acquiry start offset:                   0
Number of bytes to acquire:             29 GiB (31330402304 bytes)
Evidence segment file size:             1.4 GiB (1572864000 bytes)
Bytes per sector:                       512
Block size:                             64 sectors
Error granularity:                      64 sectors
Retries on read error:                  3
Zero sectors on read error:             no
```

```
Written: 28 GiB (30764172580 bytes) in 8 minute(s) and 43 second(s) with 56 M
iB/s (58822509 bytes/second).
MD5 hash calculated over data:          a9c40e04e11ded8e99fe6de243ed837d
ewfacquire: SUCCESS
```

Obraz dysku pomyślnie utworzony

```
Verify completed at: Dec 01, 2022 12:42:20

Read: 28 GiB (30764171264 bytes) in 2 minute(s) and 2 second(s) with 240 MiB/
s (252165338 bytes/second).

MD5 hash stored in file:                a9c40e04e11ded8e99fe6de243ed837d
MD5 hash calculated over data:          a9c40e04e11ded8e99fe6de243ed837d

ewfverify: SUCCESS
```

Obraz dysku się zgadza

```
┌──(kali㉿kali)-[~/sledcza/lab_1]
└─$ fsstat sandisk.E01
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT32

OEM Name: MSDOS5.0
Volume ID: 0x9677f7d6
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT32
Next Free Sector (FS Info): 45696
Free Sector Count (FS Info): 60040576

Sectors before file system: 2048

File System Layout (in sectors)
Total Range: 0 - 60086271
* Reserved: 0 - 3443
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 3444 - 18105
* FAT 1: 18106 - 32767
* Data Area: 32768 - 60086271
** Cluster Area: 32768 - 60086271
*** Root Directory: 32768 - 32799

METADATA INFORMATION
--------------------------------------------
Range: 2 - 960856070
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 16384
Total Cluster Range: 2 - 1876673
```

```
┌──(kali㉿kali)-[~/sledcza/lab_1]
└─$ ewfinfo sandisk.E01
ewfinfo 20140813

Acquiry information
        Case number:            1
        Examiner name:          Marcel
        Evidence number:        1
        Acquisition date:       Thu Dec  1 12:08:32 2022
        System date:            Thu Dec  1 12:08:32 2022
        Operating system used:  Linux
        Software version used:  20140813
        Password:               N/A
        Model:                  SanDisk 3.2Gen
        Serial number:          05013a1728702951763c

EWF information
        File format:            EnCase 6
        Sectors per chunk:      64
        Error granularity:      64
        Compression method:     deflate
        Compression level:      best compression

Media information
        Media type:             removable disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      60086272
        Media size:             28 GiB (30764171264 bytes)

Digest hash information
        MD5:                    a9c40e04e11ded8e99fe6de243ed837d
```

```
┌──(kali㉿kali)-[~/sledcza/lab_1]
└─$ fls -u sandisk.E01
d/d 5:  System Volume Information
d/d 7:  7-Zip
v/v 960856067:  $MBR
v/v 960856068:  $FAT1
v/v 960856069:  $FAT2
V/V 960856070:  $OrphanFiles
```

Po analizie obrazu dysku widzimy, że znajduje się na nim jedynie program 7-zip