Szymon Kozioł

ZADANIE 2:

Pytanie 1:

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

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

Pytanie 1 (mmls):

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza]
└─$ 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 Tabl
e (#0)
001:  ------    0000000000   0000000127   0000000128   Unallocated
002:  000:000   0000000128   0007581695   0007581568   Win95 FAT32
(0x0c)
```

Niealokowana pamięć znajduje się w przedziale między sektorem 0000000000, a sektorem 0000000127

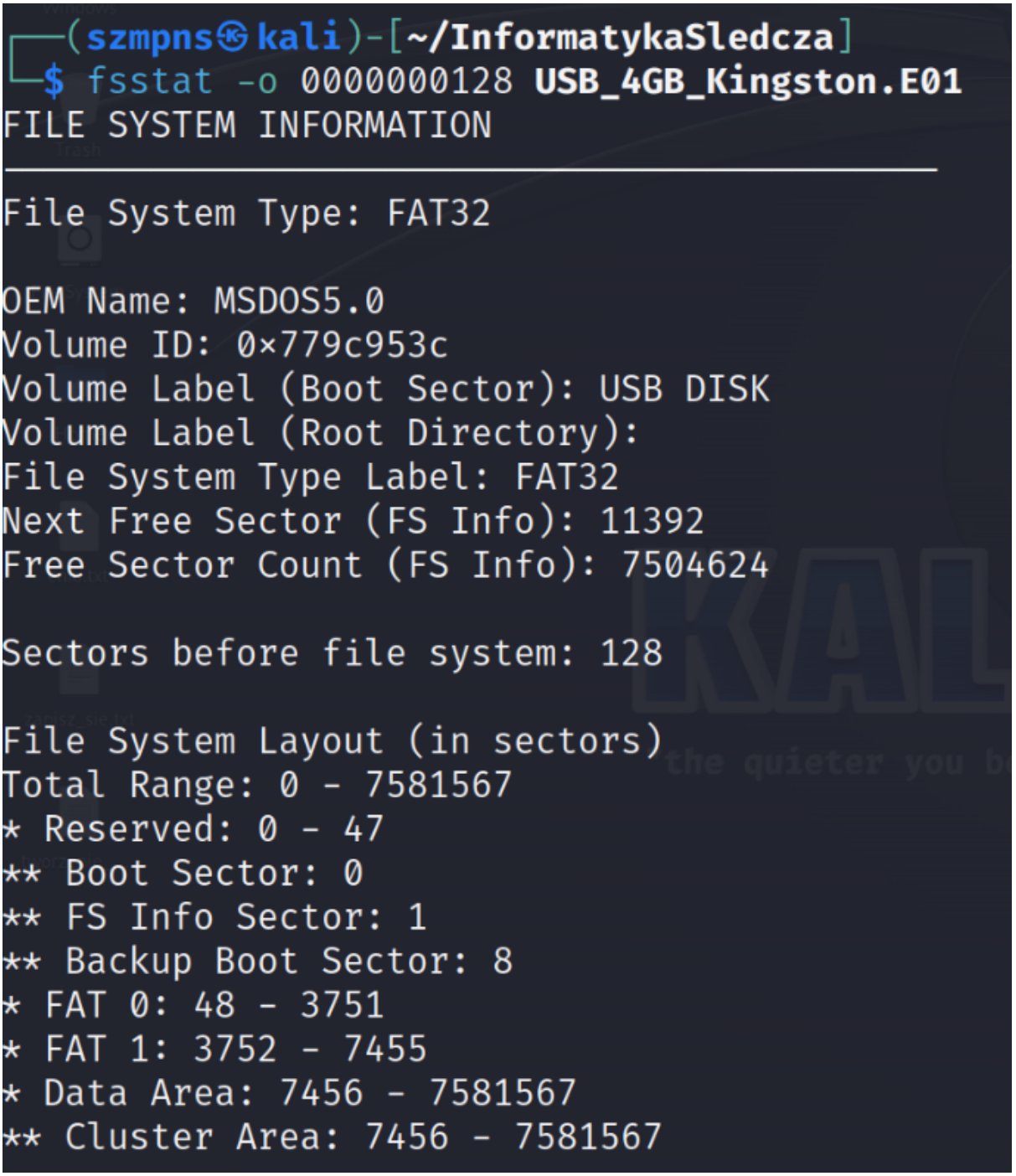
Pytanie 2:

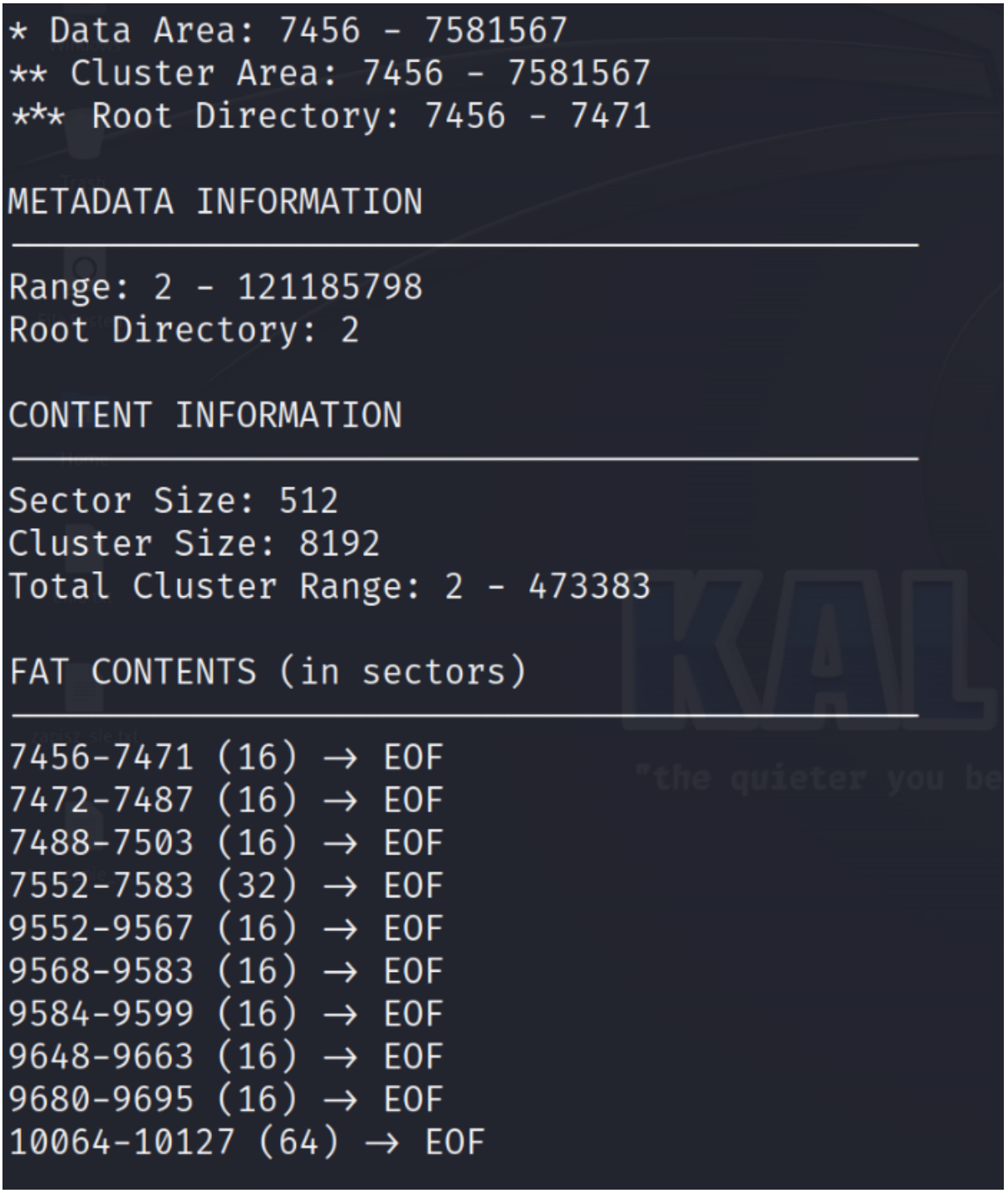
Pliki systemowe znajdują się w 2 partycji

Pytanie 3:

Początek: 0000000128
Koniec: 0007581695

Pytanie 1 (fsstat):





FAT32

Pytanie 2:

Wielkość sektora: 512 bajtów
Wielkość klastra: 8192 bajtów

Pytanie 1 (fls):

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza]
└─$ fls -p -o 0000000000128 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
```

Pytanie 2:

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza]
└─$ fls -p -o 0000000000128 USB_4GB_Kingston.E01 9
r/r 62725:      IMG_6110.JPG
r/r 62726:      IMG_5592.JPG
r/r 62727:      text.txt
```

Pytanie 1 (ewfinfo):

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza]
└─$ ewfinfo USB_4GB_Kingston.E01
ewfinfo 20140814

Acquiry information
        Case number:            001
        Examiner name:          Kali
        Evidence number:        001
        Acquisition date:       Sun Oct  3 16:31:05 2021
        System date:            Sun Oct  3 16:31:05 2021
        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 obraz dysku: Kali
Plik utworzono: 3.10.2021 o godz. 16:31:05
Numer seryjny fizycznego dysku: 0D7117891080
Nazwa modelu dysku: USB DISK 2.0
Format plików: EnCase 6
Metoda kompresji pliku: deflate
Wielkość badanego nośnika: 3881828352 bajtów
Poziom kompresji: good (fast)

ZADANIE 3:

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza]
└─$ 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
```

Pytanie 1:

Jest 1 sektor gpt_load_table

Pytanie 2:

Startowy sektor gpt_load 0: 2048

Pytanie 3:
W obrazie są dwie “strefy” niealokowanych sektorów.

1)

Start End
0000000000 0000002047

2)

Start End
0001173504 0001999999

Pytanie 4:

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza]
└─$ mmls LAB_1.img | awk '{print $1 $6 " " $7}'
GUID
Offset
Units

Slot
000:Safety Table
001:Unallocated
002:GPT Header
003:Partition Table
004:fat16
005:fat32
006:ntfs
007:ext4
008:swap
009:minix
010:Unallocated
```

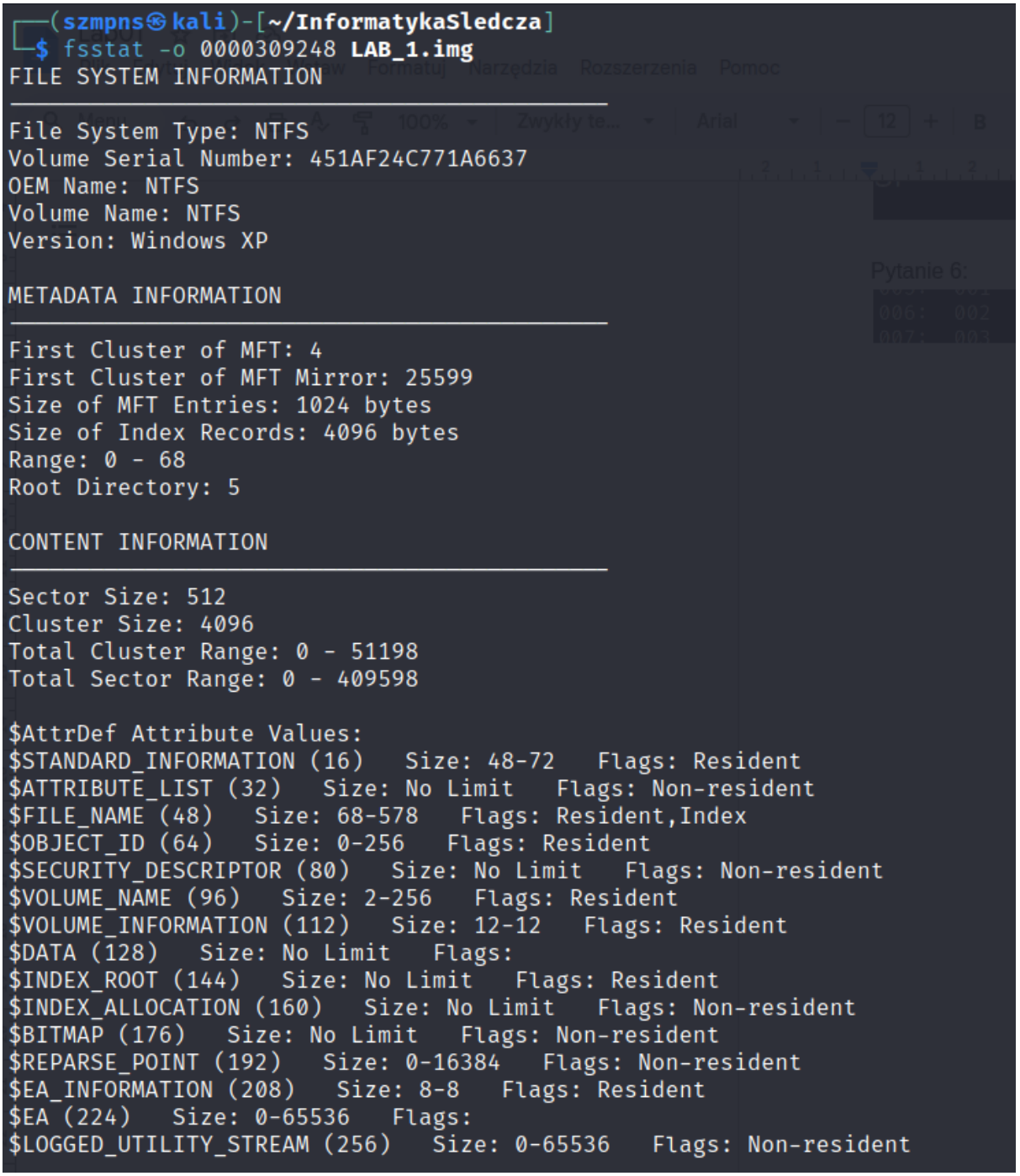
000:Safety Table
001:Unallocated
002:GPT Header
003:Partition Table
004:fat16
005:fat32
006:ntfs
007:ext4
008:swap
009:minix
010:Unallocated

Pytanie 5:

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza]
└─$ mmstat LAB_1.img
gpt
```

Pytanie 6:

```
006:  002       0000309248   0000718847   0000409600   ntfs
007:  003       0000718848   0001058815   0000339968   ext4
```



```
┌──(szmpns㉿kali)-[~/InformatykaSledcza]
└─$ fsstat -o 0000309248 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

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit   Flags: Non-resident
$VOLUME_NAME (96)   Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)   Size: No Limit   Flags:
$INDEX_ROOT (144)   Size: No Limit   Flags: Resident
$INDEX_ALLOCATION (160)   Size: No Limit   Flags: Non-resident
$BITMAP (176)   Size: No Limit   Flags: Non-resident
$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident
```

Volume Serial Number: 451AF24C771A6637

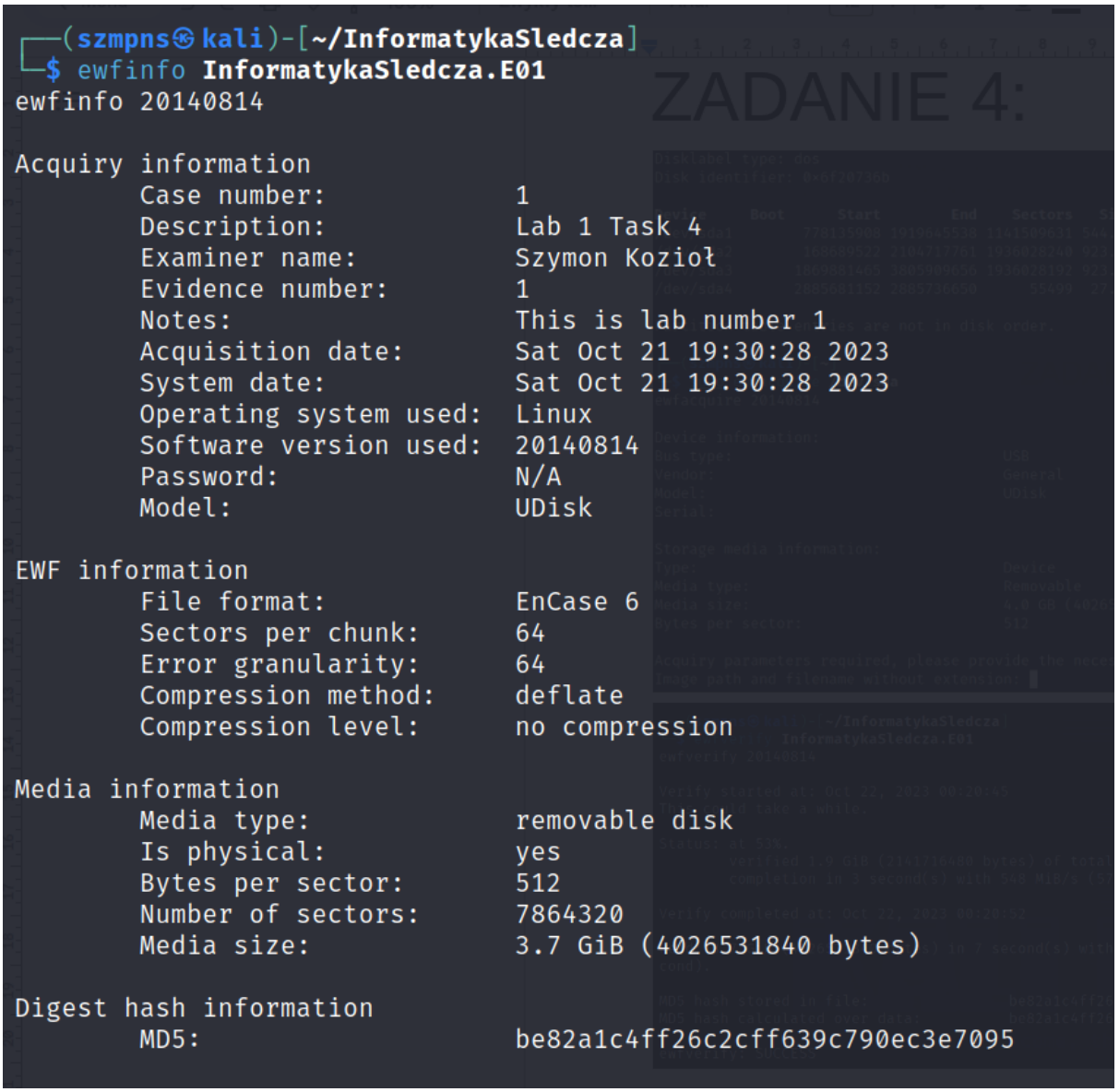
Version: Windows XP

ZADANIE 4:

```
Disklabel type: dos
Disk identifier: 0x6f20736b

Device     Boot      Start        End    Sectors   Size Id Type
/dev/sda1         778135908 1919645538 1141509631 544.3G 72 unknown
/dev/sda2         168689522 2104717761 1936028240 923.2G 65 Novell Netware 386
/dev/sda3        1869881465 3805909656 1936028192 923.2G 79 unknown
/dev/sda4        2885681152 2885736650      55499  27.1M  d unknown

Partition table entries are not in disk order.

┌──(szmpns㉿kali)-[~]
└─$ sudo ewfacquire /dev/sda
ewfacquire 20140814

Device information:
Bus type:                                       USB
Vendor:                                         General
Model:                                          UDisk
Serial:

Storage media information:
Type:                                           Device
Media type:                                     Removable
Media size:                                     4.0 GB (4026531840 bytes)
Bytes per sector:                               512

Acquiry parameters required, please provide the necessary input
Image path and filename without extension:
```

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza]
└─$ ewfverify InformatykaSledcza.E01
ewfverify 20140814

Verify started at: Oct 22, 2023 00:20:45
This could take a while.

Status: at 53%.
        verified 1.9 GiB (2141716480 bytes) of total 3.7 GiB (4026531840 bytes).
        completion in 3 second(s) with 548 MiB/s (575218834 bytes/second).

Verify completed at: Oct 22, 2023 00:20:52

Read: 3.7 GiB (4026531840 bytes) in 7 second(s) with 548 MiB/s (575218834 bytes/se
cond).

MD5 hash stored in file:                be82a1c4ff26c2cff639c790ec3e7095
MD5 hash calculated over data:          be82a1c4ff26c2cff639c790ec3e7095

ewfverify: SUCCESS
```

Ostatecznie:



```
┌──(szmpns㉿kali)-[~/InformatykaSledcza]
└─$ ewfinfo InformatykaSledcza.E01
ewfinfo 20140814

Acquiry information
        Case number:            1
        Description:            Lab 1 Task 4
        Examiner name:          Szymon Kozioł
        Evidence number:        1
        Notes:                  This is lab number 1
        Acquisition date:       Sat Oct 21 19:30:28 2023
        System date:            Sat Oct 21 19:30:28 2023
        Operating system used:  Linux
        Software version used:  20140814
        Password:               N/A
        Model:                  UDisk

EWF information
        File format:            EnCase 6
        Sectors per chunk:      64
        Error granularity:      64
        Compression method:     deflate
        Compression level:      no compression

Media information
        Media type:             removable disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      7864320
        Media size:             3.7 GiB (4026531840 bytes)

Digest hash information
        MD5:                    be82a1c4ff26c2cff639c790ec3e7095
```