Magdalena Ślusarczyk

Informatyka Śledcza

Sprawozdanie z laboratorium 5.10.2021

1. ANALIZA POBRANEGO OBRAZU (PLIK .E01).

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

```
root@pop-os:/home/madzia# md5sum  ./Desktop/sledcza/USB_4GB_Kingston.E01
b879553c628b3308d624372398d8302a  ./Desktop/sledcza/USB_4GB_Kingston.E01
root@pop-os:/home/madzia# sha1sum ./Desktop/sledcza/USB_4GB_Kingston.E01
344aa2b0179e18ad94ddcc0e5cbfa0af663faba3  ./Desktop/sledcza/USB_4GB_Kingston.E01
root@pop-os:/home/madzia#
```

1.2 W jakim przedziale sektorów znajduję się niealokowana pamięć?
Niealokowana pamięć znajduje się w sektorach od 0000000000 do 0000000127 włącznie.

1.3 W której partycji znajdują się pliki systemowe?
W partycji 002.

1.4 Proszę o podanie początku i końca sektora należącego do partycja Win95.
Początek: 0000000128 Koniec: 0007581695

```
root@pop-os:/home/madzia/Desktop/sledcza# mmls -r ./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)
```

1.5 Jaki system plików zaczyna się w sektorze 0000000128 analizowanego pliku?
FAT32

1.6 Jaka jest wielkość sektora oraz klastra w badanym obszarze?

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

1.7 Wypisz wszystkie pliki głównego katalogu USB_4GB_Kingston.E01.

```
root@pop-os:/home/madzia/Desktop/sledcza# fls -a -o 0000000128 ./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
```

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

```
root@pop-os:/home/madzia/Desktop/sledcza# fls -a -o 0000000128  ./USB_4GB_Kingston.E01 9
d/d 9:  .
d/d 2:  ..
r/r 62725:      IMG_6110.JPG
r/r 62726:      IMG_5592.JPG
r/r 62727:      text.txt
```

1.9 Pod jaki numer sprawy podlega badany nośnik?
001

Jaka jest nazwa osoby tworzącej obraz dysku?
Kali

Kiedy plik został utworzony?
Sun Oct 3 16:31:05 2021

Numer seryjny fizycznego dysku oraz nazwa modelu?
USB DISK 2.0 nr 0D7117891080

Wskaż format plików?
EnCase 6

Proszę o podanie metody kompresji pliku?
Deflate

Jaka jest pełna wielkość badanego nośnika (w bajtach)?
3881828352

Jaki poziom kompresji został wskazany przy tworzeniu pliku?
good (fast) compression

```
root@pop-os:/home/madzia/Desktop/sledcza# ewfinfo ./USB_4GB_Kingston.E01
ewfinfo 20140807

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
```

2. POZYSKANIE OBRAZU NOŚNIKA PRZY UŻYCIU NARZĘDZIA EWFACQUIRE

```
root@pop-os:~# ewfinfo /home/madzia/Desktop/sledcza/usbimage.E01
ewfinfo 20140807

Acquiry information
        Case number:            002
        Examiner name:          Magda
        Acquisition date:       Tue Oct  5 19:43:50 2021
        System date:            Tue Oct  5 19:43:50 2021
        Operating system used:  Linux
        Software version used:  20140807
        Password:               N/A

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:             fixed disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      8388607
        Media size:             3.9 GiB (4294966784 bytes)

Digest hash information
        MD5:                    c67fb2514b885331f6cf20b0c9a5f620
```